REFERENCE GUIDE FOR HAZARD ANALYSIS IN PV FACILITIES

V. M. Fthenakis
National PV EHS Assistance Center
Brookhaven National Laboratory
Upton NY 11973

S.R. Trammell
Motorola
Semiconductor Products Sector
Austin TX 78735

September 2003

Brookhaven National Laboratory
Upton, New York 11973-5000

REFERENCE GUIDE FOR HAZARD ANALYSIS IN PV FACILITIES

V. M. Fthenakis
National PV EHS Assistance Center
Brookhaven National Laboratory
Upton NY 11973

S.R. Trammell
Motorola
Semiconductor Products Sector
Austin TX 78735

September 2003

Environmental Research and Technology Division
Environmental Sciences Department

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

Managed by
Brookhaven Science Associates, LLC
for the United States Department of Energy under
Contract No. DE-AC02-98CH10886

*This work was performed under the auspices of the U.S. Department of Energy.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of author's expresses herein do not necessarily state to reflect those of the United States Government or any agency thereof.

This text should be used only as a guide and not as an ultimate source of information and guidance on Process Hazards Analysis (PHA). The purpose of this report is to complement, amplify and supplement other texts and guides on Process Hazard Analysis. The examples shown are generic ones. The processes and conditions in individual facilities may be different. The authors do not make any warrantee, express or implied, nor they assume any legal responsibility of the accuracy and completeness of any information included in this report. The user is urged to learn as much as possible about PHA and tailor the information provided herein to his or her needs.

Printed on recycled paper

TABLE OF CONTENTS

ABSTRACT

Photovoltaic manufacturing facilities use toxic, corrosive or flammable substances, which, if not handled properly can present environmental, health and safety (EHS) risks. Although the amounts of hazardous substances used in the PV industry are far smaller than those used in the chemical industry, such substances can present EHS hazards. As PV manufacturing is scaled-up to meet a growing demand, preserving the safe and friendly to the environment nature of PV becomes even more important. This paper presents systematic methods of hazard evaluation and accident prevention that are available to the industry. These methods include checklists, what if analysis, hazard and operability analysis (HazOp), failure modes and effects analysis (FEMA), event tree analysis, fault tree analysis (FTA), layers of protection analysis (LOPA), safety analysis reviews (SAR) and security risk analysis. The strengths and weaknesses of each method are discussed, and sample applications in PV manufacturing are presented. The costs of conducting hazard analyses and implementing associated corrective actions were only moderate; the expected benefits by far surpass the associated costs. Such analyses, in addition to enhancing the safety of a facility, they can also lead to improvements in reliability and productivity.

1. INTRODUCTION

A comprehensive approach for accident prevention and minimization of EHS risks includes several layers of protection. Administrative & engineering options to prevent accidental releases and reduce their consequences should be considered sequentially in several steps; each one adding a layer of protection. The first step is to consider inherently safer technologies, processes and materials. For processes where hazardous materials can not be avoided, safer delivery and use of materials must be sought (e.g. liquid vs. pressurized gas, reduced on-site inventories, high material utilization and on-demand generation).

Once specific materials and systems have been selected, strategies to prevent accident-initiating events need to be evaluated and implemented. Facilities that handle highly hazardous chemicals above certain threshold quantities are required to comply with the Occupational Safety and Health Administration (OSHA) Process Safety Management (PSM) Rule and the Environmental Protection Agency (EPA) Risk Management Program (RMP). The OSHA PSM rule focuses on accident prevention, whereas the EPA RMP expands beyond prevention to the mitigation of the consequences of an accident. About 180 materials are presently listed in these rules; some of these materials are used in PV manufacturing. Most of today's PV facilities are not subject to compliance with these rules because they handle quantities smaller than the threshold quantities. Nevertheless, a pro-active approach on minimizing risks is to the utmost advantage of the PV industry and, the OSHA and EPA provisions should taken as guidance for all PV facilities that handle highly hazardous materials. Perhaps the most important item in the PSM rule is the process-hazard analysis (PHA). Hazard analyses focus on equipment, instrumentation, utilities, human actions and external factors that might impact the process and cause an accident- initiating event.

Several hazard analysis methods are available. Guidelines for using hazard analysis in the chemical industry are published by the American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS). Also, Sematech has published a Hazard Analysis Guide for semiconductor manufacturing equipment. This current reference guide aims in assisting EHS professionals in photovoltaic manufacturing in selecting and using a method for analyzing hazards. To this end, in addition to giving a general overview of methods, we present examples of hazard analysis directly applicable to PV manufacturing, and we discuss the level of effort and lessons learnt for each of the examples. This text should be used only as a guide and not as an ultimate source of information and guidance on process hazard analysis. Information on this topic will be periodically updated and feedback provided by the reader will be appreciated.

The reader does not need to read the whole report. Section 2 provides an overview of the common hazard analysis methods. This section can help you to determine which method is applicable to analyzing your process. Then you can go directly to the section of the report that describes the method you want to study. For additional information you can contact the authors (email: vmf@bnl.gov; Steve.Trammell@motorola.com).

2. OVERVIEW OF HAZARD ANALYSIS TECHNIQUES

The purpose of process hazard analysis (PHA) is to determine if credible accident initiating events exist and to define corrective actions. PHA considers planed and unplanned actions and events, related to both systems and human interactions. Several hazard analysis methods are available, ranging from simple questionnaires to fully blown quantitative analysis. In general, the required level of effort and the sophistication of the analysis needed, reflect the complexity of the process.

All hazard analyses are team activities. The team should include individuals that understand well the system and a facilitator who is organized and can draw the participation and contributions of the employees. The team composition is as important as the technique itself. PHA methods range from the simple Checklist or What if analyses that require only a few hours of meetings to the very comprehensive FTA that may require months of effort.

2.1 Checklists

A checklist comprises guidelines in bullet or question form to assist a methodical EHS inspection of a process and to stimulate thinking and discussion. Checklists are developed by experts who have conducted many hazard analyses, in conjunction with experts in the process being reviewed. A checklist will include safety items specified by codes, regulations and industry safety practices. Checklists are very useful when conducting a safety self-appraisal or audit of a process or facility.

A checklist of suggested safe practices for the storage, distribution, use and disposal of hazardous gases in photovoltaic manufacturing is included as Appendix A[1]. A checklist applicable to equipment installation is included as Appendix B[1]. No checklist is complete or ultimately comprehensive; however, efforts must be made to ensure that no obvious issues are overlooked. This is the limitation of checklists; they can only help identify the obvious (to the expert) EHS weaknesses in a process or equipment. For studying potential interactions between different types of systems and procedures that could lead to an accident, we need additional methods of analysis.

2.2 What If Analysis

The “What if” analysis is a method of brainstorming where people familiar with the process ask questions about possible undesirable events. Through the questioning process, experienced people can identify accident situations and their consequences, evaluate existing safeguards and suggest risk reductions measures. The degree of thoroughness in the application of this method is largely dependent upon the team composition. It is a powerful technique when the staff is experienced. Yet, it is a simple method, which can produce results in a few hours of meetings. It is useful for relatively simple systems, but may not help in identifying the potential for multiple failures or

[1] Electronic versions of these checklists are available from the authors. These are evolving documents and comments or suggestions for updating or enhancing them would be appreciated.

synergistic effects. The process is qualitative and risk or consequence ranking is not accomplished. Details on the use of the What If Analysis are given in Section 4.

2.3. HazOp Analysis

HazOp is a structured analysis of a system, process unit or operation, with the goal to identify accident-initiating scenarios. The HazOp team conducts a step-by-step examination of a design and intent of a system or operation. The system to be studied is divided to sections (nodes) that provide a logical breakdown of major subsystems for examination. For example, a typical chemical vapor deposition (CVD) process may be divided to the following nodes: gas panel, liquid delivery system, process reactor, vacuum pump, and pollution control system. The method requires the review of documentation documents, including drawings (PIDs and PFDs), component specifications, and logical control programs. HazOp utilizes a set of guidewords (e.g., none, more, high), in combination with the system parameters to seek physically possible deviations from the design intent (e.g., no flow, high pressure or high temperature). The team concentrates on those deviations that could lead to potential EHS risks. The analysis aims in being systematic and rigorous yet open and creative. When causes of a deviation are found, the team screens the potential consequences based on their experience; for consequences with undesirable potential, consequence analysis tools (e.g., atmospheric dispersion models, blast analysis models) are used to quantify the level of consequences.

For a HAZOP to be successful, the design must be well developed and firm. If the drawings are incomplete or inaccurate, the study would be worthless. The boundaries (nodes) of the study must be clearly analyzed and studied. A clear description and design intent must be given to every section of the design, which is analyzed. As with all PHA methods, the study team must be well chosen to combine knowledge and experience.

2.4 Failure Mode and Effects Analysis

A Failure Modes and Effects Analysis (FMEA) is applicable in the analysis of equipment which is made up of components with well-defined failures. An FMEA will start with tabulating the failure modes of equipment and their effects on the system the equipment is part of or are interacting with.. A failure mode describes how a piece of equipment fails (e.g., open, closed, leaking). The effect of the failure mode is determined by the system's response to the equipment failure. FMEA aims in identifying single failure modes that could either result in or contribute significantly to an accident. Human factors (i.e. operator error) are usually not examined directly in an FMEA, but the effect of an operation error is represented by an equipment failure mode.

FEMA is the method of choice of the automobile industry. For example Ford Motor company requires their suppliers to perform detailed FMEAs on all designs and processes they provide. Also, the semiconductor industry is increasingly requiring from their equipment supplier FMEAs of new pieces of equipment or system designs. Similarly, the PV manufacturing industry should require from their suppliers that FMEA should be done, at the minimum, at the functional level of new equipment. FMEA in addition to being a method of hazard analysis, examines equipment reliability to ensure that the equipment meets customer needs.

The purpose of an FMEA is to identify single equipment and system failure modes; it is not designed to identify an exhaustive list of combination of equipment failures that could lead to an accident. For such application, a combination of HazOp/FMEA is instrumental. The exercise will start with a HazOp to determine causes of system failure. Then the team will select the failure modes that need individual study and will employ FMEA to tabulate deviations, causes and consequences. Subsequently a numerical risk ranking system can be used to evaluate and rank recommendations for corrective actions.

2.5 Event Tree Analysis (ETA)

An event tree is a graphical representation of the possible outcomes of an accident-initiating event (e.g., a failure of a specific equipment or procedure). Event tree analysis can be used to identify accidents that may occur in a complex system. An event tree can be constructed by a single analyst who has a detailed knowledge of the system, but a team approach is preferred, since it promotes brainstorming that can produce a more complete analysis.

After the individual accident sequences are identified by an ETA, the specific combinations that could lead to an accident can be determined using Fault tree Analysis.

2.6 Fault Tree Analysis (FTA)

Fault tree analysis can be used to determine failure sequences and failure probabilities of complex and undesirable events, *such as major fire* ***and*** *failure of automatic fire protection system,* and to understand their possible causes in terms of more basic events, *such as loss of electrical power to firewater system,* and even more basic events, such as *power cable damaged in fire.*

A fault tree is a picture of the logical relationships between the primary events (e.g., failures of specific components), the intermediate events (e.g., failure of one part of a safety system as a function of failures of various components), and the top event (e.g., failure of containment and release to the environment). To construct a fault tree, the failure of interest is designated as a top event. Tracing backwards, all failures that could lead to the top event are identified. This process continues until failures are reached that cannot be reduced any more, or cannot be quantified. This set of logical relationships can be processed using Boolean algebra to provide a logical expression relating the top event to combinations of primary events. In one form of this expression, each term is a combination of primary events that is a **minimal cut set:** *a combination that is sufficient to cause the top event*. Given the likelihood of the primary events, this expression can serve as a basis for quantifying the likelihood of the top event, and it contains a great deal of information about the causes of the top event.

FTA is useful in particular contexts, which are characterized below:

Hypothetical Consequences of an Accident are Unacceptable
If a facility handles a large quantity of hazardous substances, and the potential consequences of an accident are extremely undesirable, then a comprehensive hazard analysis is warranted. The systematic nature of FTA is particularly valuable in this context, and the relatively high level of effort associated with FTA can be justified.

Safety Case for a Facility Depend on Multiple Layers of Defense (Safety Systems, Fire Extinguishing Systems, Plant Trip Logic, etc.)
Multiple layers of defense exist at some facilities handling potentially hazardous materials, such that a release requires failure or bypass of these layers of defense. The reason for having multiple layers is that if they are independent, failure of all of them can be made extremely unlikely. Under rather simple assumptions, it can be argued that two layers failing with probabilities of 10^{-3} each is an easier design to realize than one layer at 10^{-6}, because 10^{-6} is an extremely small failure probability that cannot be easily supported in light of phenomenological uncertainty, common cause, etc. Therefore, a common strategy is to go for multiple layers of defense, each reasonably unlikely to fail, in the hope that failure of the combination is essentially incredible. This hope is only realized if the layers are completely independent. Much of the reason for undertaking fault tree analysis boils down to the need to look for circumstances that compromise the hypothetical independence of redundant layers of defense. In particular, it is necessary to be on the lookout for conditions that adversely affect a given layer of defense at the same time that they produce a safety challenge to that layer (e.g., a fire that takes out a fire suppression system or a loss of electrical power that simultaneously creates a plan transient and deprives a mitigating system of power).

Complex Systems
The failure modes associated with all but the simplest systems are too complex to study without the aid of computers. Fault trees are a simple and unambiguous way to organize a comprehensive logic model for computer analysis.

2.7 Safety Analysis Review (SAR)

SAR is a simplified form of risk assessment. It typically uses orders of magnitude for quantifying the frequency of an accident-initiating event, the consequence severity, and the likehood of failure of independent protection layers. By combining probability and consequence categories, an approximate (relative) risk estimate is obtained. This method can use the information developed during a What If or HazOp analysis. The primary role of SAR is to identify accident-initiating scenarios and determine if sufficient layers of protection exist to safeguard against each accident scenario. SARs are usually conducted for R&D or chemical laboratory environments where several small-scale operations may be hosted in the same building.

2.8 Layers of Protection Analysis (LOPA)

Similarly to SAR, LOPA is a simplified form of risk assessment. It also uses order of magnitude categories for initiating event frequency, consequence severity, and the likehood of failure of independent protection layers. By combining probability and consequence categories, an approximate (relative) risk estimate is obtained. The primary role of LOPA is to determine if there are sufficient layers of protection against an accident scenario. It is best applied as a further review of protective layers based on failure scenarios developed from initial qualitative hazard analysis studies (e.g., HazOp). The larger the potential consequences the more layers of protection are needed.

2.9 Security Risk Analysis

In response to the events of September 11, many companies stepped up security efforts in chemical facilities and other installations. Since resources are limited, a system for ranking relative risk is useful in establishing priorities for implementing physical-security infrastructure and programs. Security Risk Analysis (SRA) is an assessment of relative risk that can augment conventional process hazard analysis. SRA is based on categorizing threat, vulnerability, and the consequences of deliberate actions by terrorists, disgruntled employees, and others. Order of magnitude ranking is used for each of these categories and the produced risk matrix can be used to assign priorities to actions for correcting deficiencies. Details of this analysis are given in Section 10.

In the following we present illustrative examples of applying hazard analyses to processes in photovoltaic manufacturing and we discuss associated costs and lessons learnt.

3. “WHAT IF” ANALYSIS

3.1 Methodology Overview

The “What if” analysis is a brainstorming approach in which a group of people familiar with the process ask questions or voice concerns about possible undesirable events. The questions are asked in the form of “What if” related to equipment or other system failures, and procedural errors. For example: “What if power to the exhaust blower X is lost?”, or “what if relief valve Y fails to open?” Through the questioning process, experienced people can identify accident situations and their consequences, evaluate existing safeguards and suggest risk reductions measures. The degree of thoroughness in the application of this method is largely dependent upon the team composition. It is a powerful technique when the staff is experienced. The team must include at least one person with good knowledge of the process. Typically it involves a process engineer, maintenance engineer and a safety and/or environmental specialist. A person who is skilled in the analysis should be the leader of this activity. For simple systems, 2 or 3 people with interdisciplinary background may be assigned to perform the analysis of each process station.

The team must be well organized to ensure that the “what if” questions were exhausted. This is a simple method, which can produce results in a few hours of meetings. It is useful for relatively simple systems, but may not help in identifying the potential for multiple failures or synergistic effects.

What If is the less structured of the hazard analysis methods described in this report. The relatively free, creative atmosphere may pose a challenge to the team leader because he/she has less control on the discussion. Below we list some recommendations for the leader that would assist in conducting a successful analysis.

1. Schedule the meeting at a convenient time and place. One or two ½ day meetings should suffice for most processes.
2. Seek the active participation of experienced personnel.
3. Include people who know about past incidents, near misses, and safety concerns.
4. Send each team member a summary of the process and pertinent information a week or two before the meeting, and ask them to prepare some What–if questions before the review. (The team discussions will prompt other ideas and concerns; however, some homework before the meeting usually helps).
5. Prepare a preliminary list of What-if questions to ask at the meeting.
6. Keep the discussion in track and be prepared to ask What-if questions if the discussion becomes idle.
7. The team should not be allowed to try solving problems during the What if brainstorming. (Team members should generate What if questions w/o worrying about responses).
8. Encourage people to examine possible deviations from the design, construction, modification, or operating intent of the process.
9. Record all the questions on a board or a spreadsheet.

10. Divide the questions into specific areas of investigation (e.g., fire protection, gas safety, industrial hygiene).
11. Give the questions' worksheet to all participants to develop responses
12. Open discussion on the responses, and seek consensus on each response
13. Present the results a tabular form that includes the questions, their consequences and recommendations
14. Recommendations need to be assigned and their implementation should be tracked weekly until all the recommendations are addressed.

Ground Rules for All Team Members

1. All team members will have equal say.
2. Any concern, no matter how inconsequential it appears, can be suggested.
3. Spin-off questions and ideas are encouraged.
4. All team members are expected to contribute.
5. Detailed analysis and criticism of questions and ideas is not allowed
6. The focus of the brainstorming sections is to identify hazards, not to find solutions.
7. Suggestions and recommendations will follow up for those questions that the team finds credible.
8. All the team members will have the opportunity to review the issues and recommendations before they are given to the facility manager.

3.2 What-If / Checklist Analysis

"What if" can be used in conjunction with checklists to combine previous experience with brainstorming regarding new and/or different concerns. For this purpose a checklist is useful even if it is incomplete, because the What-If portion of this method encourages the team to consider potential accident initiating events that are beyond the experience compiled in the spreadsheet. The checklist items would prompt team members to ask questions that could reveal hazardous situations. The team usually generates a table of potential accident initiating scenarios, effects, safeguards, and action items. The results of this analysis may also help in enhancing a checklist.

Usually the What If and What If/Checklist methods will require fewer people and shorter meetings than does a more structured technique such as HAZOP Analysis, FMEA or FTA.

4. HAZARD AND OPERABILITY STUDY (HAZOP)

4.1 Methodology Overview

HazOp is a mature methodology, with system failure mode identification as its strength. By dividing complex systems into smaller more manageable "nodes" for study, and the systematic identification of process parameter deviations, it makes for a thorough identification of system failure modes. The HazOp method utilizes a team to perform the assessment, and the team typically consists of system operators, maintenance specialists, design or equipment engineers, EHS and facility engineers and a person who is knowledgeable of the HazOp methodology.

4.2 HazOp Example Applications

Example 1: Bulk Chemical Delivery System.

In this application, a design-phase HazOp study was performed on a factory wide bulk chemical delivery system. HazOp was selected as the analysis method because the system has distinct components, yet continuous process flow with interacting system parameters. Since the operational components have their own defined operating parameters, it was relatively simple to divide the system into 3 separate study nodes. The equipment involved in this study included the bulk chemical dispense storage and pumping unit, the valve box distribution units, and the piping system. (See PID in Appendix 1). These three main sub-systems became the study nodes, from which process deviations, causes and undesired consequences were evaluated. (Figure 1.1).

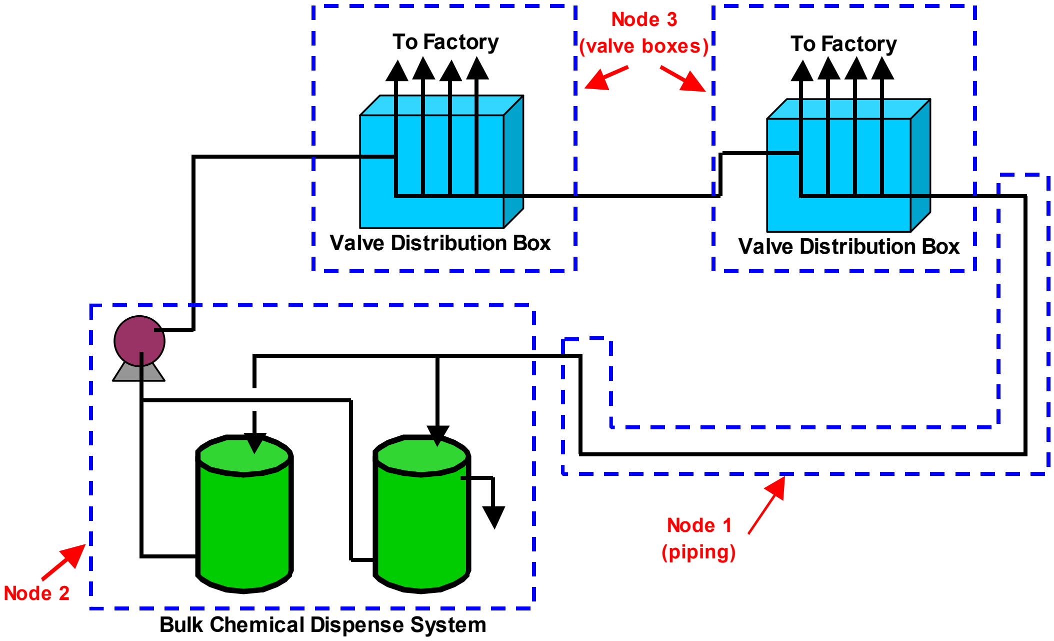
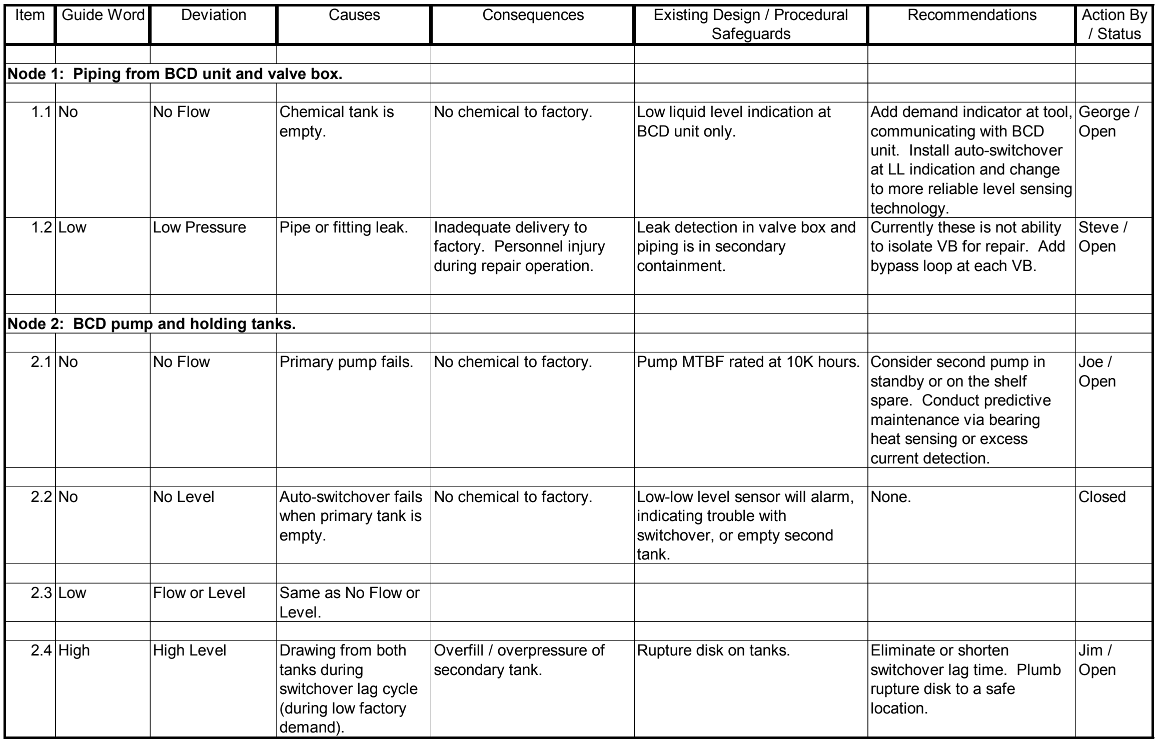


Figure 4.1: Bulk Chemical Delivery System Simplified Schematic

Lessons Learned.

Several important design and operational issues were discovered during this study, and were documented on the HazOp worksheet (Figure 1.2).



Item	Guide Word	Deviation	Causes	Consequences	Existing Design / Procedural Safeguards	Recommendations	Action By / Status
Node 1: Piping from BCD unit and valve box.							
1.1	No	No Flow	Chemical tank is empty.	No chemical to factory.	Low liquid level indication at BCD unit only.	Add demand indicator at tool, communicating with BCD unit. Install auto-switchover at LL indication and change to more reliable level sensing technology.	George / Open
1.2	Low	Low Pressure	Pipe or fitting leak.	Inadequate delivery to factory. Personnel injury during repair operation.	Leak detection in valve box and piping is in secondary containment.	Currently these is not ability to isolate VB for repair. Add bypass loop at each VB.	Steve / Open
Node 2: BCD pump and holding tanks.							
2.1	No	No Flow	Primary pump fails.	No chemical to factory.	Pump MTBF rated at 10K hours.	Consider second pump in standby or on the shelf spare. Conduct predictive maintenance via bearing heat sensing or excess current detection.	Joe / Open
2.2	No	No Level	Auto-switchover fails when primary tank is empty.	No chemical to factory.	Low-low level sensor will alarm, indicating trouble with switchover, or empty second tank.	None.	Closed
2.3	Low	Flow or Level	Same as No Flow or Level.				
2.4	High	High Level	Drawing from both tanks during switchover lag cycle (during low factory demand).	Overfill / overpressure of secondary tank.	Rupture disk on tanks.	Eliminate or shorten switchover lag time. Plumb rupture disk to a safe location.	Jim / Open

Figure 4.2: Bulk Chemical Dispense System HazOp Worksheet

An overview of the most significant of these are as follows:

- **Node 1: Piping from BCD unit and valve box.**
  - No flow to factory due to low liquid detection failure within main chemical tank. This deviation was considered a likely event due to the historic high failure rates of float type level indicators in this service. Only a local alarm is provided within the BCD system, and it is dependent upon the operator to acknowledge this alarm and respond appropriately. Also, there is a reasonable potential that the chemical tank could be near its low alarm level when a high tool demand occurs. In this case, the operator is given only a very short response time to switch the feed line to the secondary tank, before the primary tank is emptied.
    - Corrective Action: For the majority of tools, a demand signal was programmed into the existing system logic to allow for direct communication with the BCD system. An auto-switchover function was added to allow non-operator assisted switchover to the secondary chemical supply tank upon activation of the level indicator. A pair of capacitance type probes, which provided higher reliability in this service, and a redundant signal in the event one of the probes failed, replaced the level indicator.

- Low pressure (and inadequate delivery to the factory) due to major pipe or fitting leaks. This deviation was considered probable due to leakage issues in similar pressurized chemical delivery systems. Upon review of the potential leak locations, it was discovered that there was no provision for isolating some sections of the system (specifically the valve manifold boxes) to allow for safe repair or maintenance.
    - Corrective Action: A bypass loop and block valves were added at each valve manifold box to allow for system isolation in the event that a leak repair was required.

- **Node 2: Bulk chemical dispense pump and holding (storage) tanks.**
    - No flow to the factory due to failure of the primary BCD system pump. The pump manufacturer states a Mean Time Between Failure (MTBF) of this pump at a relatively high reliability of 10,000 hours. However, since there is only a single pump in service and schedule preventive maintenance intervals are highly variable (due to short and infrequent factory down time windows), pump failure was considered a high-risk issue.
        - Corrective Actions: Initially a PM interval of .75 MTBF minimum was scheduled, to allow for variability in the actual window of opportunity to perform maintenance. Consideration was given to installing an in-line spare, however physical space inside the BCD cabinet was not available. It was finally determined that predictive maintenance could be performed via heat sensing at the critical bearings and monitoring of current draw on the pump motor.

    - High level (high pressure) within one of the chemical tanks during switchover lag cycle combined with low factory demand. There is a 10-minute lag time during switchover from a chemical tank at low level to the second full tank, during which time product is drawn from both tanks simultaneously. If during this time there happens to be low or no factory demand for chemical, all of the product is recirculated and returns to only one of the storage tanks. There is a potential that the return tank will be receiving more product that is being pumped out, thereby overfilling and overpressurizing the vessel. This scenario was considered of low probability since a combination of events would need occur simultaneously, however the consequence was of high enough significance for the item to be studied.
        - Corrective Actions: The switchover time was shortened to further drive down the likelihood of an event. A rupture disk was added to the tank, the discharge from which was piped to an external drain.

Level of Effort.

As described, a HazOp study is a team approach for evaluating hazards of a system. In this study, a facilitator who was familiar with the HazOp methodology led the analysis meetings and a scribe was assigned to record the meeting results. The team consisted of a process engineer, a maintenance engineer, a representative from the company supplying the bulk chemical dispense equipment, an EHS engineer and two chemical system operators. The facilitator and scribe participated in all of the meetings, with the system experts attending the majority of the time and during sessions where their expertise was needed. Meetings were held in ½ day increments, and on four separate days. An estimate of the labor hours expended on this effort is detailed in Figure 1.3.

Participant	Hours
Facilitator	36
Scribe	28
EHS Engineer	16
Process Engineer	10
Maintenance Engineer	12
Equipment Representative	12
Operator 1	12
Operator 2	16
	Total: 142

Figure 4.3: BCD HazOp Labor Hours

Costs to Implement Recommendations.

The estimated costs associated with implementing the key HazOp recommendations are shown in Figure 1.4. In several cases, no costs were incurred since only operating procedures were affected, or equipment and system design changes were incorporated prior to final design and specification of equipment.

Item	Recommendation	Approx. Cost of Implementation
1.1	Add demand indicator at tool, communicating with BCD unit. Install auto-switchover at Low Level indication and change to more reliable level sensing technology.	None for tools as the communication protocols were added to design specification. $2500 for level sensor upgrade.
1.2	Add bypass loop at each valve box.	$1500 for valves and piping.
2.1	Conduct predictive maintenance via bearing heat sensing or excess current detection.	None. Procedure change only.
2.4	Eliminate or shorten switchover lag time. Plumb rupture disk to a safe location.	None. Programming change only. Rupture disk and piping added to equipment design specification.

Figure 4.4: Implementation Costs for BCD HazOp Recommendations

Example 2: Sulfuric Acid Reprocessing System

In this application, a system HazOp study was performed on a sulfuric acid reprocessing system. Again, a HazOp was selected as the analysis method because the system has distinct components yet continuous process flow with interacting system parameters. Since the operational components have their own defined operating parameters, it was relatively simple to divide the system into 4 separate study nodes. Reprocessing of bulk chemicals is becoming more popular as the costs of these high quality manufacturing chemicals increases. In some cases, reprocessing also provides a higher quality of material and strict operational controls can result in lower likelihood of introducing contaminates into the process. This reprocessing system consists of an acid concentrator unit (ACU) which takes the spent acid from the factory and removes the excess water, the acid reprocessing unit (ARU) which repurifies the acid to the specified concentration, and the Sampler and Distribution Unit (SDU), which conducts an on-line evaluation of acid quality, then distributes the acid to either the qualified acid tanks, or routes off-spec material back to the recovery tank. (See PID in Appendix 2) The recovery tank collects both off-spec material and acid returned from the factory. A simplified system layout is depicted in Figure 1.4.

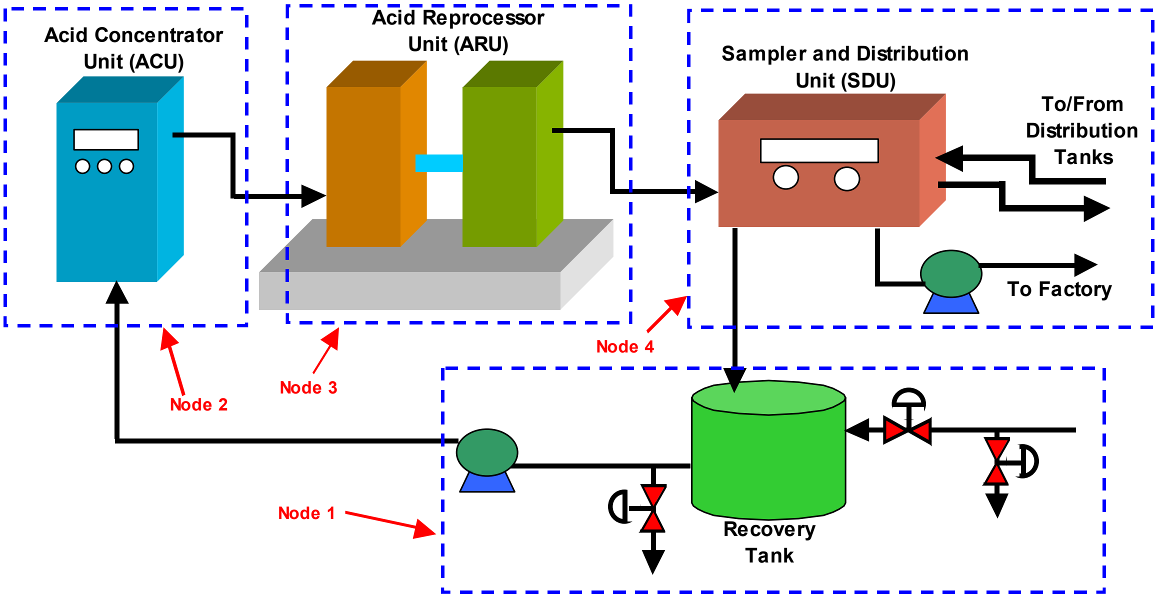
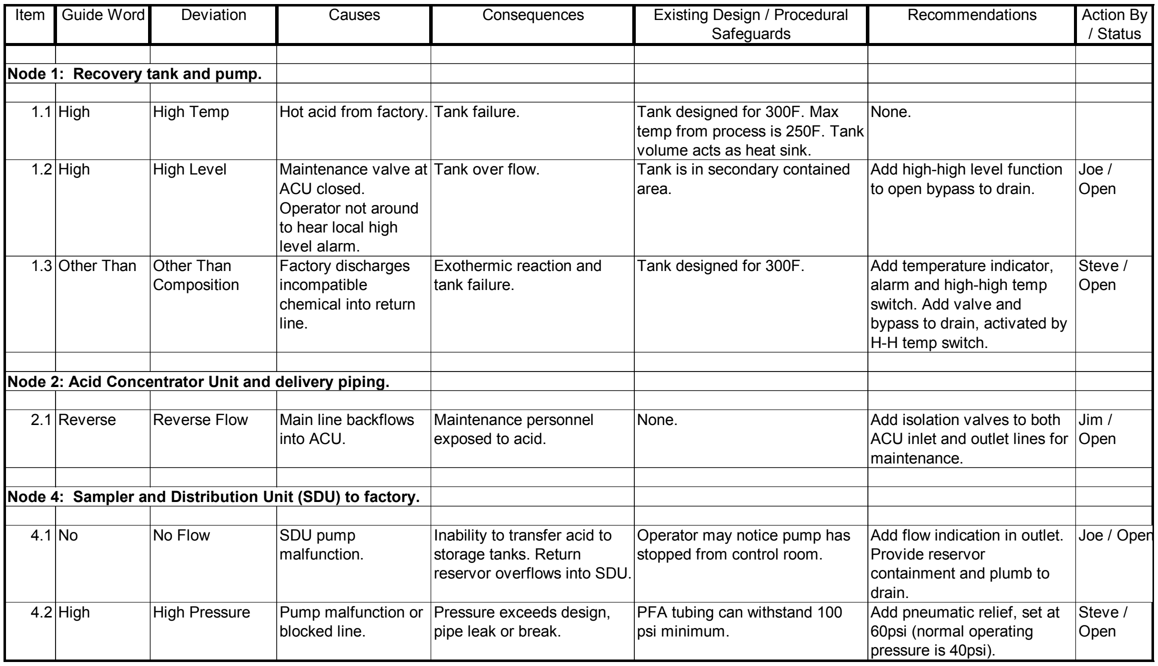

Acid Concentrator Unit (ACU)
Acid Reprocessor Unit (ARU)
Sampler and Distribution Unit (SDU)
To/From Distribution Tanks
To Factory
Node 1
Node 2
Node 3
Node 4
Recovery Tank

Figure 4.5: Acid Reprocessing System Schematic

Lessons Learned.

Several important design and operational issues were discovered during this study, and were documented on the HazOp worksheet (Figure 1.5).



Item	Guide Word	Deviation	Causes	Consequences	Existing Design / Procedural Safeguards	Recommendations	Action By / Status
Node 1: Recovery tank and pump.							
1.1	High	High Temp	Hot acid from factory.	Tank failure.	Tank designed for 300F. Max temp from process is 250F. Tank volume acts as heat sink.	None.	
1.2	High	High Level	Maintenance valve at ACU closed. Operator not around to hear local high level alarm.	Tank over flow.	Tank is in secondary contained area.	Add high-high level function to open bypass to drain.	Joe / Open
1.3	Other Than	Other Than Composition	Factory discharges incompatible chemical into return line.	Exothermic reaction and tank failure.	Tank designed for 300F.	Add temperature indicator, alarm and high-high temp switch. Add valve and bypass to drain, activated by H-H temp switch.	Steve / Open
Node 2: Acid Concentrator Unit and delivery piping.							
2.1	Reverse	Reverse Flow	Main line backflows into ACU.	Maintenance personnel exposed to acid.	None.	Add isolation valves to both ACU inlet and outlet lines for maintenance.	Jim / Open
Node 4: Sampler and Distribution Unit (SDU) to factory.							
4.1	No	No Flow	SDU pump malfunction.	Inability to transfer acid to storage tanks. Return reservor overflows into SDU.	Operator may notice pump has stopped from control room.	Add flow indication in outlet. Provide reservor containment and plumb to drain.	Joe / Oper
4.2	High	High Pressure	Pump malfunction or blocked line.	Pressure exceeds design, pipe leak or break.	PFA tubing can withstand 100 psi minimum.	Add pneumatic relief, set at 60psi (normal operating pressure is 40psi).	Steve / Open

Figure 4.6. Acid Reprocessing System HazOp Worksheet

An overview of the most significant of these is as follows:

- **Node 1: Acid recovery tank and pump.**
    - High level in recovery tank due to a blockage in pump discharge line. The most credible cause for line blockage was a closed maintenance valve on the inlet side of the ACU. Since the ACU is the most maintenance intensive component in the reprocessing system, it was judged likely that this condition would occur several times over the life of the facility. The tank is in a bermed area, however overflow of the tank would increase the risk of personnel exposure for both system operators and spill response teams. Also, the overflow could be significant if not immediately observed by the day shift personnel (evening and night shifts only conduct occasional walk-through inspections during these shifts).
        - Corrective Action: A high-high level function was added to the recovery tank, which was designed to open a valve and drain materials to the industrial waste treatment plant. A liquid leak detection device was placed in the tank secondary containment, to indicate and alarm in the presence of liquid.

    - Exothermic reaction in the tank due to the discharge of incompatible materials into the drain lines from the factory. Although the tank is rated for 300F service, it is believed that incompatible reactions could result in temperatures significantly above the tank design temperature.
        - Corrective Action: A temperature indicator, alarm and a high-high temperature switch were added. This switch would open a drain

valve near the tank inlet, allowing bypass of the incompatible mixture into the industrial waste drain.

- **Node 2: Acid concentrator unit and delivery piping.**
  - Main line backflows into the ACU (reverse flow) and potential for maintenance personnel to be exposed to acid.
    - Corrective Actions: Isolation valves for maintenance were added to both the inlet and outlet lines. These would provide for safe shutdown of any of the components and allow for preventive maintenance or repair.

- **Node 4: Sampler and distribution unit to factory.**
  - No flow in the system due to a SDU internal pump malfunction. This would result in the inability to transfer acid to the storage tanks. It was determined that this event, if unobserved for an extended time, would result in loss of chemical to the factory.
    - Corrective Actions: Flow indication in the outlet (pump discharge) was added, and an alarm signal would be sent to the security station.

  - High pressure in the system due to a pump malfunction or a blocked line. This would result in a possible line leak or break. The tubing is designed to withstand a minimum of 100psi, however it is expected the pump discharge could easily exceed this pressure if blocked.
    - Corrective Actions: It was determined that normal operation pressure of the system is approximately 40psi. Pneumatic relief was added to the system as the first component downstream of the pump, to relieve high pressure (set at 60 psi). The relief piping was plumbed to the industrial waste drain.

Level of Effort.

In this study, a facilitator who was familiar with the HazOp methodology led the analysis meetings and a scribe was assigned to record the meeting results. The team consisted of a process engineer, a manufacturing engineer, a quality engineer, a maintenance engineer, a representative from the company supplying the reprocessor equipment, an EHS engineer and one system operator. The facilitator and scribe participated in all of the meetings, with the system experts attending the majority of the time and during sessions where their expertise was needed. Meetings were held in ½ day increments, and on seven separate days. An estimate of the labor hours expended on this effort is detailed in Figure 1.6.

Participant	Hours
Facilitator	52
Scribe	44
EHS Engineer	20
Process Engineer	20
Manufacturing Engineer	12
Quality Control	20
Maintenance Engineer	28
Equipment Operator	28
Operator	20
	Total: 244

Figure 4.7: Reprocessor HazOp Labor Hours

Costs to Implement Recommendations.

The estimated costs associated with implementing the key HazOp recommendations are shown in Figure 1.7. In several cases, no costs were incurred since only operating procedures were affected, or equipment and system design changes were incorporated prior to final design and specification of equipment.

Item	Recommendation	Approx. Cost of Implementation
1.2	Add high-high level function to open bypass to drain.	None. Existing sensor was able to accommodate 2nd signal input therefore only programming changes are necessary.
1.3	Add temperature indicator, alarm and high-high temperature switch. Add valve and bypass to drain, activated by H-H temperature switch.	$7500 for additional equipment and electronics.
2.1	Add isolation valves to both ACU inlet and outlet lines for maintenance.	$750 for valves.
4.1	Add flow indication in outlet. Provide reservoir containment and plumb to drain.	$2000 for additional equipment and electronics.
4.2	Add pneumatic relief, set at 60psi (normal operating pressure is 40psi).	None. Pump specification was changed to include a model with an integral relief valve.

Figure 4.8: Implementation Costs for Reprocessor HazOp Recommendations

5. FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

5.1 Methodology Overview

FMEA is a mature methodology, which tabulates failure modes of equipment or systems and determines their effects on the overall process. The method is used by taking a specific component or section of an engineered system, evaluating it for possible failure modes, and uses structured evaluation protocols (such as a risk matrix or numerical scale) to judge the effects of the failure mode, likelihood of occurrence and existence of current controls. FMEA studies can be performed by an individual knowledgeable of the methodology (with specific inputs from selected system experts), but is more effectively performed by a team (similar to HazOp). The team approach to FMEA typically includes system operators, maintenance specialists, design or equipment engineers, EHS and facility engineers and a facilitator who is familiar with the methodology. An FMEA can be used in a semi-quantitative manner, which assists in establishing relative risks among the identified failure scenarios and determining priorities for application of corrective actions. (See Appendix 3 for an example of a FMEA scoring chart).

5.2 FMEA Examples

Example 1: Chemical Vapor Deposition Tool Exhaust System

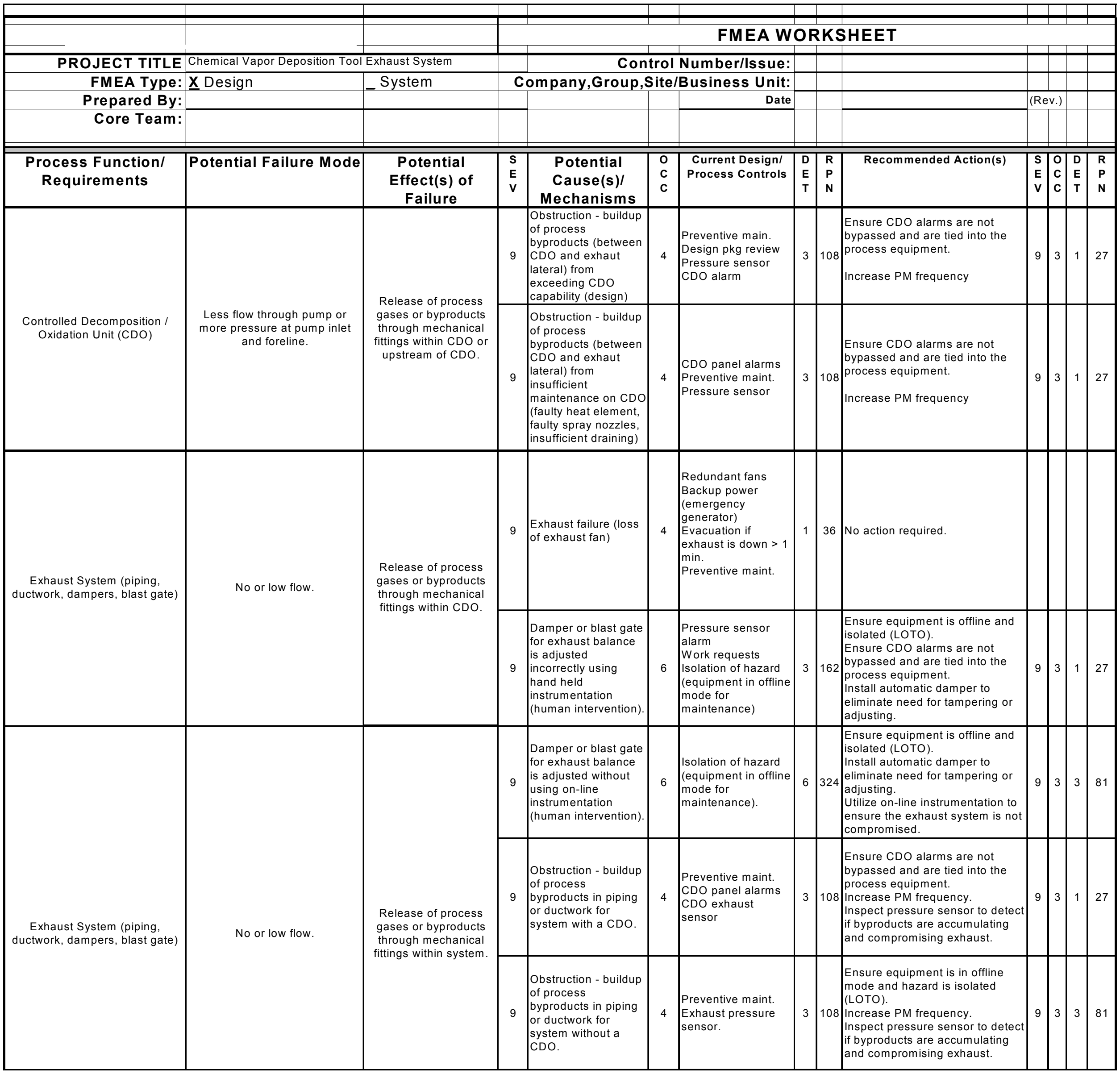
In this example, an evaluation of the exhaust system on a typical chemical vapor deposition (CVD) process was performed. Concern had been raised of a potential post-plasma release of process gases and byproducts from the exhaust system. The FMEA was conducted to determine failure modes within the exhaust system that might result in these releases. FMEA was the method of choice since the study was focused on a relatively small and specific section of the tool exhaust system.

Lessons Learned.
Several important design and operational issues were discovered during this study, and were documented on the FMEA worksheet (Figure 2.1).

Overviews of the most significant of these are as follows:

- **Controlled Decomposition / Oxidation Unit (CDO).**
    - The failure mode of less flow through the vacuum pump or more pressure at the vacuum pump inlet and foreline was determined to be a credible event caused by a variety of potential obstructions in the system. These causes were categorized into two areas; buildup of process byproducts because the CDO capability has been exceeded, and buildup of byproducts due to insufficient maintenance. In both cases, existing process controls of preventive maintenance schedules, pressure sensors and a variety of CDO alarms were identified, however none were of sufficient reliability to reduce risk below an acceptable level.

- Recommendations: Although the CDO contains a significant number of alarm functions, the alarm system is relatively simple to bypass. With concurrence of the equipment manufacturer, all alarm bypass capability within the CDO was eliminated. Additionally, the pressure sensor located in the upstream duct was tied into the CDO alarm panel, and functionality was added to the system to prevent tool startup if any CDO system was in an alarm state.



FMEA WORKSHEET

PROJECT TITLE	Chemical Vapor Deposition Tool Exhaust System		**Control Number/Issue:**		
FMEA Type:	X Design	_ System	**Company,Group,Site/Business Unit:**		
Prepared By:			**Date**		(Rev.)
Core Team:					

Process Function/ Requirements	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Potential Cause(s)/ Mechanisms	OCC	Current Design/ Process Controls	DET	RPN	Recommended Action(s)	SEV	OCC	DET	RPN
Controlled Decomposition / Oxidation Unit (CDO)	Less flow through pump or more pressure at pump inlet and foreline.	Release of process gases or byproducts through mechanical fittings within CDO or upstream of CDO.	9	Obstruction - buildup of process byproducts (between CDO and exhaust lateral) from exceeding CDO capability (design)	4	Preventive main. Design pkg review Pressure sensor CDO alarm	3	108	Ensure CDO alarms are not bypassed and are tied into the process equipment. Increase PM frequency	9	3	1	27
			9	Obstruction - buildup of process byproducts (between CDO and exhaust lateral) from insufficient maintenance on CDO (faulty heat element, faulty spray nozzles, insufficient draining)	4	CDO panel alarms Preventive maint. Pressure sensor	3	108	Ensure CDO alarms are not bypassed and are tied into the process equipment. Increase PM frequency	9	3	1	27
Exhaust System (piping, ductwork, dampers, blast gate)	No or low flow.	Release of process gases or byproducts through mechanical fittings within CDO.	9	Exhaust failure (loss of exhaust fan)	4	Redundant fans Backup power (emergency generator) Evacuation if exhaust is down > 1 min. Preventive maint.	1	36	No action required.				
			9	Damper or blast gate for exhaust balance is adjusted incorrectly using hand held instrumentation (human intervention).	6	Pressure sensor alarm Work requests Isolation of hazard (equipment in offline mode for maintenance)	3	162	Ensure equipment is offline and isolated (LOTO). Ensure CDO alarms are not bypassed and are tied into the process equipment. Install automatic damper to eliminate need for tampering or adjusting.	9	3	1	27
Exhaust System (piping, ductwork, dampers, blast gate)	No or low flow.	Release of process gases or byproducts through mechanical fittings within system.	9	Damper or blast gate for exhaust balance is adjusted without using on-line instrumentation (human intervention).	6	Isolation of hazard (equipment in offline mode for maintenance).	6	324	Ensure equipment is offline and isolated (LOTO). Install automatic damper to eliminate need for tampering or adjusting. Utilize on-line instrumentation to ensure the exhaust system is not compromised.	9	3	3	81
			9	Obstruction - buildup of process byproducts in piping or ductwork for system with a CDO.	4	Preventive maint. CDO panel alarms CDO exhaust sensor	3	108	Ensure CDO alarms are not bypassed and are tied into the process equipment. Increase PM frequency. Inspect pressure sensor to detect if byproducts are accumulating and compromising exhaust.	9	3	1	27
			9	Obstruction - buildup of process byproducts in piping or ductwork for system without a CDO.	4	Preventive maint. Exhaust pressure sensor.	3	108	Ensure equipment is in offline mode and hazard is isolated (LOTO). Increase PM frequency. Inspect pressure sensor to detect if byproducts are accumulating and compromising exhaust.	9	3	3	81

Figure 5.1: CVD Tool Exhaust FMEA Worksheet

- **Exhaust System (piping, ductwork, dampers, blast gate):**
  - No or low flow within the exhaust system resulting in byproduct release within the CDO was determined to be a credible event cause by

catastrophic exhaust failure (loss of the exhaust fan), or incorrect adjustment of the damper or blast gate. The loss of exhaust fan failure mode scenario was deemed to have highly reliable controls since there exists a redundant in-line fan and backup emergency power for the system. Therefore, no additional actions were required for this item. For the damper and blast gate scenario, it was determined that a potential existed for incorrect adjustment (resulting in low flow) due to errors in operating the hand-held static pressure measurement instrument, or incorrect calibration of the instrument itself.

  - Recommendations: In addition to eliminating the CDO bypass function, it was recommended that the manual damper be replaced with an automatic damper, which would be designed to fail in the open position. This would eliminate the human error potential and lower the overall risk into an acceptable range.

- No or low flow within the exhaust system with gas or byproduct release through mechanical fittings was determined to be a credible event caused primarily by the incorrect damper or blast gates adjustment, or by an obstruction within the piping or ductwork. An additional scenario, which could result in a gas release, is the intentional removal of the pump foreline (during a maintenance activity) without isolation of the system.
  - Recommendations: Previous recommendations of eliminating the CDO bypass function, tying the CDO alarm signal to the tools to prevent startup while in an alarm mode, and installation of automatic dampers all apply to reduce the risk of this scenario. One additional recommendation was to install a system interlock on the vacuum pump foreline piping which would activate an alarm if the vacuum system is compromised while any of the system equipment was in operation.

Level of Effort.

For this FMEA effort, the lead analyst prepared a sizable portion of the document, and assembled a small team of appropriate experts to finalize several sections of the analysis. The FMEA meeting was held in one 6-hour session, and included the lead analyst as the facilitator, a maintenance engineer, a process engineer and an EHS engineer. A scribe was also present to record information generated in the session. Estimates of the labor hours expended on this effort are detailed in Figure 2.2.

Participant	Hours
Analyst/Facilitator	40
Scribe	8
EHS Engineer	12
Process Engineer	6
Maintenance Engineer	6
	Total: 72

Figure 5.2: Tool Exhaust FMEA Labor Hours

Costs to Implement Recommendations.

The estimated costs associated with implementing the key FMEA recommendations are shown in Figure 2.3. In several cases, no costs were incurred since only operating procedures were affected, or equipment and system design changes were incorporated prior to final design and specification of equipment.

Potential Failure Mode	Recommendation	Approx. Cost of Implementation
Less flow through pump or more pressure at inlet.	Ensure alarms are not bypassed. Increase PM frequency. Pressure sensor tied into CDO panel.	None. Procedural change only. Slight increase in maintenance costs due to increasing PM frequency. Minor costs (wiring) for pressure sensor tie-in (CDO alarm capability in place).
No or low flow (gas leak within CDO).	Ensure equipment is off line during maintenance (locked out), and alarms are not bypassed. Install automatic damper valves (vs. manual valves).	No cost for procedural changes. $7500 for installation of automatic dampers and control system.
No or low flow (gas leak within system outside of CDO).	Ensure equipment is off line during maintenance (locked out). Install automatic damper valves (vs. manual valves). Install on-line instrumentation to ensure system is not compromised.	No cost for procedural changes. $7500 for installation of automatic dampers and control system. $3500 for on-line instrumentation.
No or low flow (gas leak within system outside of CDO).	Ensure alarms are not bypassed. Increase PM frequency. Inspect pressure sensor for byproduct accumulation.	None. Procedural change only. Slight increase in maintenance costs due to increase in inspection frequency and added inspection for pressure sensor.
No or low flow (gas leak within system outside of CDO).	Ensure equipment is off line during maintenance (locked out). Increase PM frequency. Inspect pressure sensor for byproduct accumulation.	None. Procedural change only. Slight increase in maintenance costs due to increase in inspection frequency and added inspection for pressure sensor.

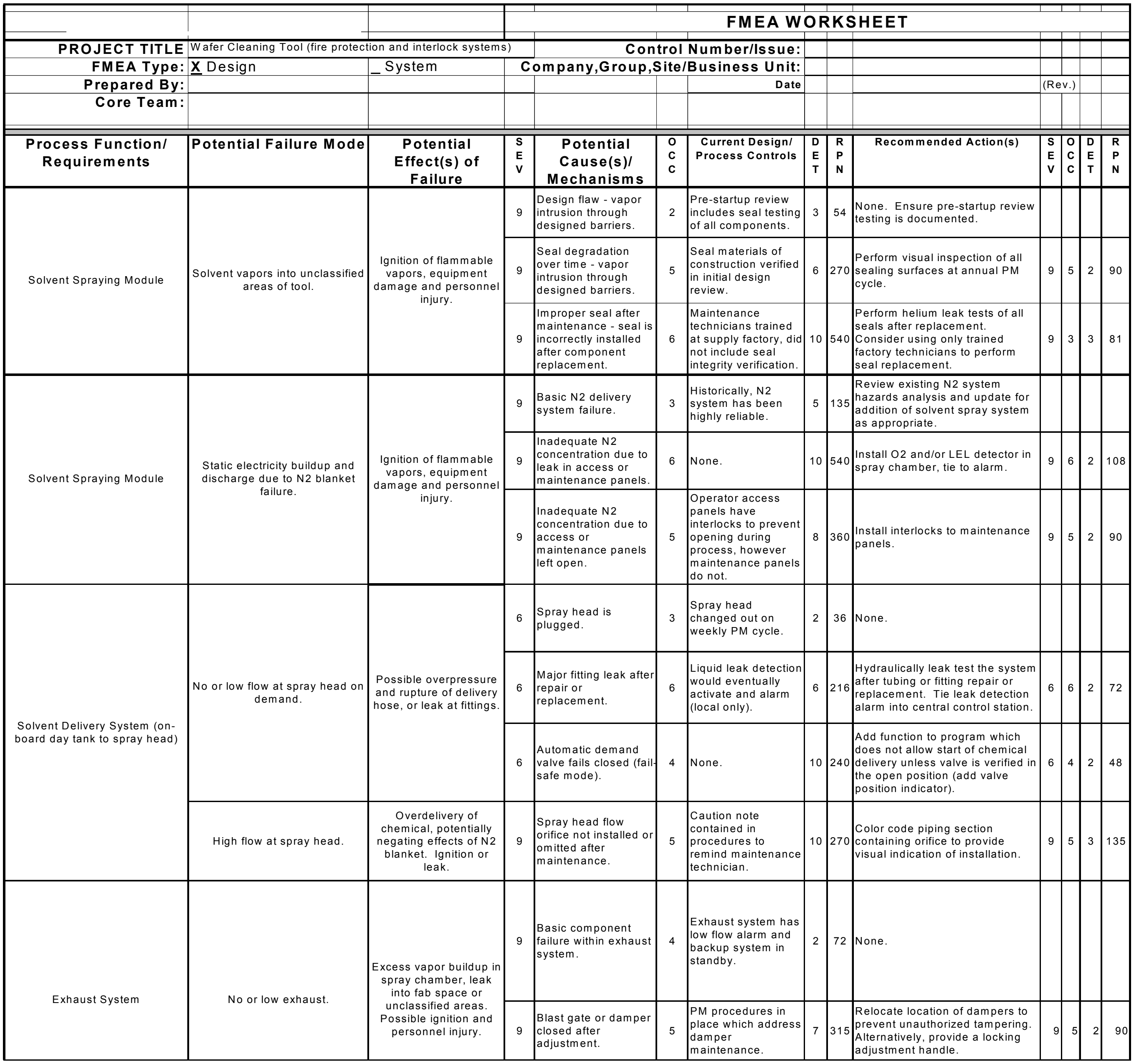
Figure 5.3: Implementation Costs for Tool Exhaust FMEA Recommendations

Wafer Cleaning Tool (fire protection and interlock system study)

In this example, an evaluation of a wafer-cleaning tool was performed. This cleaning system utilized heated solvent to strip contaminates and residual films from prior processing steps. Since the potential risks associated with heated and vaporized solvents are high, a specific FMEA was conducted and focused on the adequacy of two major safety systems, fire protection and interlocks. The FMEA approach was the method of choice since the evaluation was centered on a specific piece of equipment and would focus on component failures.

Lessons Learned.

Several important design and operational issues were discovered during this study, and were documented on the FMEA worksheet (Figure 5.4).



			FMEA WORKSHEET										
PROJECT TITLE	Wafer Cleaning Tool (fire protection and interlock systems)					Control Number/Issue:							
FMEA Type:	X Design	_ System	Company,Group,Site/Business Unit:										
Prepared By:						Date				(Rev.)			
Core Team:													
Process Function/ Requirements	**Potential Failure Mode**	**Potential Effect(s) of Failure**	**SEV**	**Potential Cause(s)/ Mechanisms**	**OCC**	**Current Design/ Process Controls**	**DET**	**RPN**	**Recommended Action(s)**	**SEV**	**OCC**	**DET**	**RPN**
Solvent Spraying Module	Solvent vapors into unclassified areas of tool.	Ignition of flammable vapors, equipment damage and personnel injury.	9	Design flaw - vapor intrusion through designed barriers.	2	Pre-startup review includes seal testing of all components.	3	54	None. Ensure pre-startup review testing is documented.				
			9	Seal degradation over time - vapor intrusion through designed barriers.	5	Seal materials of construction verified in initial design review.	6	270	Perform visual inspection of all sealing surfaces at annual PM cycle.	9	5	2	90
			9	Improper seal after maintenance - seal is incorrectly installed after component replacement.	6	Maintenance technicians trained at supply factory, did not include seal integrity verification.	10	540	Perform helium leak tests of all seals after replacement. Consider using only trained factory technicians to perform seal replacement.	9	3	3	81
Solvent Spraying Module	Static electricity buildup and discharge due to N2 blanket failure.	Ignition of flammable vapors, equipment damage and personnel injury.	9	Basic N2 delivery system failure.	3	Historically, N2 system has been highly reliable.	5	135	Review existing N2 system hazards analysis and update for addition of solvent spray system as appropriate.				
			9	Inadequate N2 concentration due to leak in access or maintenance panels.	6	None.	10	540	Install O2 and/or LEL detector in spray chamber, tie to alarm.	9	6	2	108
			9	Inadequate N2 concentration due to access or maintenance panels left open.	5	Operator access panels have interlocks to prevent opening during process, however maintenance panels do not.	8	360	Install interlocks to maintenance panels.	9	5	2	90
Solvent Delivery System (on-board day tank to spray head)	No or low flow at spray head on demand.	Possible overpressure and rupture of delivery hose, or leak at fittings.	6	Spray head is plugged.	3	Spray head changed out on weekly PM cycle.	2	36	None.				
			6	Major fitting leak after repair or replacement.	6	Liquid leak detection would eventually activate and alarm (local only).	6	216	Hydraulically leak test the system after tubing or fitting repair or replacement. Tie leak detection alarm into central control station.	6	6	2	72
			6	Automatic demand valve fails closed (fail-safe mode).	4	None.	10	240	Add function to program which does not allow start of chemical delivery unless valve is verified in the open position (add valve position indicator).	6	4	2	48
	High flow at spray head.	Overdelivery of chemical, potentially negating effects of N2 blanket. Ignition or leak.	9	Spray head flow orifice not installed or omitted after maintenance.	5	Caution note contained in procedures to remind maintenance technician.	10	270	Color code piping section containing orifice to provide visual indication of installation.	9	5	3	135
Exhaust System	No or low exhaust.	Excess vapor buildup in spray chamber, leak into fab space or unclassified areas. Possible ignition and personnel injury.	9	Basic component failure within exhaust system.	4	Exhaust system has low flow alarm and backup system in standby.	2	72	None.				
			9	Blast gate or damper closed after adjustment.	5	PM procedures in place which address damper maintenance.	7	315	Relocate location of dampers to prevent unauthorized tampering. Alternatively, provide a locking adjustment handle.	9	5	2	90

Figure 5.4. Spray Solvent Tool FMEA Worksheet

- **Solvent Spraying Module:**
  - Solvent vapors entering into an unclassified area of the tool was considered a credible failure mode, caused by several mechanisms involving sealing surfaces. Effects of these failures was potential ignition of the vapors, which would result in equipment damage and personnel injury. The mechanism of most concern for this failure mode was incorrect installation of a seal after a maintenance operation. Although the maintenance technicians were trained at the supplier factory, there was no

training nor written specification for replacement of the seal or requirement for seal integrity verification.

    - A recommendation for developing seal integrity verification procedures was added. This included a requirement for conducting helium leak checks, performed by trained supplier representatives.

- **Solvent Spraying Module:**
  - Static electricity buildup and discharge due to the failure of the N2 inerting system was considered a credible failure mode. The potential effect was ignition of flammable vapors, equipment damage and personnel injury. Causes for this failure mode were issues with the N2 delivery system or inadequate concentration of N2 due to leakage from improperly sealed maintenance panels. During this study, it was determined that there was no control in place to detect inadequate concentrations of N2 within the module.
    - Corrective Actions: A recommendation to add a N2 or LEL sensor within the spray module was added. Also discussed was the need to add interlocks to the maintenance access panels to prevent system startup in the event that the panels were not closed or replaced properly.

- **Solvent Delivery System (on-board day tank to spray head):**
  - No or low flow at the solvent spray head, due to a major fitting leak or valve failures was considered as credible events. The effect of these failures could be overpressure or rupture of the delivery hose, or a major solvent leak at the fittings. The only control in place for this event would be existing leak detection within the tools, which would initiate a local alarm.
    - Corrective Actions: Requirements to leak test the piping system after replacement or repair was added, and the leak detection alarm function was upgraded to transmit the leak detection alarm signal to the central control station. The equipment control system and valve type was changed to include a function, which would prohibit the start of chemical flow unless the valve position indicator verified that the valve was in the correct position.

  - High flow at the spray head was also reviewed as a potential failure mode. The only cause determined for this failure mode was the incorrect installation of the spray head or restrictive orifice after a maintenance procedure. Maintenance to clean the spray heads is frequently required to prevent plugging, which could result in improper spray patterns, therefore this event was considered a credible cause.
    - Corrective Actions: The spray head was redesigned to include the restrictive orifice as an integral part, therefore eliminating the potential for omitting the orifice during installation. Also, the

piping section containing the spray head was color coded such that the correct installation of this piece could be verified by visual inspection.

Level of Effort.

For this FMEA effort, a team approach was used to conduct the majority of the analysis. The lead analyst pre-prepared most of the FMEA study sheets, and assembled a team of experts to finalize the analysis. The FMEA meeting was held in five 4-hour sessions, and included the lead analyst as the facilitator, a maintenance engineer, a process engineer an EHS engineer and two equipment manufacturing representatives (one design engineer and one EHS engineer). A scribe was also present to record information generated in the session. An estimate of the labor hours expended on this effort is detailed in Figure 2.5.

Participant	Hours
Analyst/Facilitator	60
Scribe	30
EHS Engineer	20
Process Engineer	20
Maintenance Engineer	20
Equipment Rep. (design)	20
Equipment Rep. (EHS)	20
	Total: 190

Figure 5.5: Spray Tool FMEA Labor Hours

Costs to Implement Recommendations.

The estimated costs associated with implementing the key FMEA recommendations are shown in Figure 2.6. In several cases, no costs were incurred since only operating procedures were affected, or equipment and system design changes were incorporated prior to final design and specification of equipment.

Potential Failure Mode	Recommendation	Approx. Cost of Implementation
Solvent vapors into unclassified area of tool.	Perform visual inspection of sealing surfaces. Perform helium leak checks after seal replacement. Use factory reps to install seals.	Visual inspections and helium leak check procedure adds 1 hour of labor during each maintenance cycle.
Static electricity buildup and discharge due to N2 blanket failure.	Install O2 or LEL detector. Install interlocks on maintenance panels.	$5000 for installation of detector and electronics. $1500 per interlock (tool cost increase due to spec change).
No or low flow at spray head on demand.	Leak test after maintenance. Upgrade leak detection circuit to alarm at control station.	Leak test procedure will add 2 hours of labor during each maintenance cycle. $3000 to upgrade circuit.
High flow at spray head.	Color code piping section to indicate correct installation.	Minor costs associated with color coding of piping.
No or low exhaust.	Relocate location of dampers to prevent tampering, or replace handle with one, which can be locked in place.	$2500 for damper relocation. $200 to upgrade handle section to lockable type.

Figure 5.6: Implementation Costs for Solvent Tool FMEA Recommendations.

FMEA Scoring Chart

SCORE	Severity		Occurrence	Detection - Process	Detection - Procedure
	Severity is a rating corresponding to the seriousness of an effect of the potential failure mode. **[IN THE ABSENCE OF DETECTION]**		**Occurrence is an evaluation of the rate at which a first level cause and the failure mode will occur, with standard preventive maintenance.** [1,2,3,4] **[IN THE ABSENCE OF DETECTION]**	**Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence.** [2,5,6]	**Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence.** [7]
	EHS	**Facilities**			
1	No effect on people. No regulatory compliance impacts.	No production impact. Process utility in spec. System or equipment or operations failures can be corrected after an extended period.	Failure barely plausible $>1 \times 10^{-6}$ (1 event in more than 100 years)	Redesign of process eliminating hazard. Rescore RPN for new hazard. *Example: Replacing toxic process chemical with non-toxic chemical.*	Elimination of human based process. *Example: Replace procedure with automated process (which should be separately assessed for risk).*
2	People will probably not notice the failure. Nuisance effects.	No production impact. Process utility in spec. System or equipment or operations failure can be corrected at next scheduled maintenance.	Failure unlikely in similar processes or products. No industry history of failure. $<1x10^{-6}$ (1 event in 100 years)	Automatic controls highly likely to predict a failure mode and initiate automatic response, preventing the failure mode. *Example: Pressure sensor modifies process conditions to prevent overpressure that would have caused leak.*	Control and release of hazardous energy, with written procedure and independent verification. *Example: Block and bleed of high pressure fluid pipeline, with written procedures and supervisor inspection.*
3	Minor short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected ASAP.	Remote chance of failures. (1 event every couple of decades)	Automatic controls likely to predict a failure mode and initiate manual response, preventing the failure mode. *Example: Pressure sensor activates alarm initiating prepared response plan to prevent overpressure that would have caused leak.*	Control of hazardous energy, with written procedure and independent verification. *Example: Block of high pressure fluid pipeline, with supervisor inspection.*
4	Moderate short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected immediately.	Very few failures likely. $<1x10^{-6}$ (1 event in 10 years)	Automatic controls likely to detect the failure mode and initiate automatic response, preventing the consequence. *Example: Redundant pH probe in wastewater treatment system, preventing out of control reagent feed.*	Control and release of hazardous energy with written procedures and without independent verification. *Example: Block and bleed of high pressure fluid pipeline, without supervisor verification.*
5	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. NOV unlikely.	No production impact. Process utility our of spec. No tool impact. No product scrap.	Few failures likely. (1 event every few years)	Manual controls likely to predict the failure mode and initiate manual response, preventing the consequence. *Example: Routine inspection based parametric monitoring program with defined repair program.*	Control of hazardous energy, with written procedure and without independent verification. *Example: Block of high pressure fluid pipeline, without supervisor inspection.*
6	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. NOV likely.	Localized production impact confirmed or likely. Critical process utility out of spec. One or more production tools impacted. Possible product scrap.	Occasional failures. $<1x10^{-4}$ (1 event per year)	Automatic controls likely to detect the failure mode and initiate automatic response, lessening the consequence. *Example: Ambient air gas sensor activating process shutdown, thereby minimizing leak.*	Cell left blank intentionally to clarify the safety gap between tasks performed with control of hazardous energy and those without control of hazardous energy.
7	Significant but self-recovering effects to people or environment. Moderate extended non-compliance. NOV certain.	Widespread production outage <8 hrs. Critical process utility outage <4hrs or severely out of spec <4 hrs. Product scrap likely.	Moderate number of failures. (1 event every few months)	Automatic controls likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Exterior leak sensor activates alarm initiating prepared response plan to limit volume of leak.*	No control of hazardous energy, with written procedures and independent oversight. *Example: Electrical hot-work with partner.*
8	Significant but remediable effects to people or environment. Significant long term non-compliance NOV and media attention certain.	Widespread production outage <24 hrs. Critical process utility outage 4-12 hrs or severely out of spec 4-12 hrs. Substantial product scrap likely.	Frequent failures likely. $<1x10^{-3}$ (1 event every 1.5 months)	Manual controls fairly likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Routine inspections, with parametric monitoring, with defined measurement thresholds requiring repair.*	No control of hazardous energy, with written procedures and without oversight. *Example: Electrical hot-work without partner.*
9	Probably major injury to people or environment. Regulatory action including fines and process shutdown likely.	Widespread production outage < 48 hrs. Critical process utility outage 12-24 hrs. or moderate contamination of cleanroom or process utility. Substantial product scrap likely.	High number of failures. (1 event every few weeks)	Manual controls might randomly detect failure mode and initiate manual response, lessening the consequence. *Example: Routine walk-by inspections, without parametric monitoring, with defined observed conditions requiring repair.*	Control of hazardous energy, without written procedure.
10	Probably severe injury to people or environment. Regulatory action including fines and process shutdown certain.	Widespread production outage >48 hrs. Critical process utility outage>24 hrs or severe contamination of cleanroom or process utility. Substantial product scrap likely.	Failure certain to occur in near future. Some company or industry history. $<1x10^{-2}$ (2 or more events per week)	Controls unlikely to detect the failure mode. *Example: Device fails silent or device not routinely inspected/observed.*	No control of hazardous energy and no written procedures.

1. Failure rates are assumed to apply to continuous processes. Intermittent equipment operational failure rates may be higher due to start up failure, failure to operate at specification, and/or human error.
2. Controls involving design "hardening" (such as stronger materials of construction) are equivalent to QS9000 Type 1 controls and thereby modify Occurrence.
3. If industry average failure rates used and preventive maintenance is less frequent that manufacturer's recommendation, add 1 to Occurrence score.
4. If industry average failure rate used and proven predictive maintenance is utilized, subtract 1 from Occurrence score.
5. Controls that only detect consequence rate a 10 for detection.
6. The reliability of automatic systems and manual procedures is assumed very high. Otherwise, these systems should be assessed separately.
7. The term "hazardous energy" is intended to represent any hazard, including electrical, hydraulic, mechanical (e.g. sharp edge), radiation, chemical, etc.

Cell Color Key:

Inherently safer design/passive controls.

Highest order active controls.

Generally adequate active controls.

Human based active controls.

No controls.

6. EVENT TREE ANALYSIS (ETA)

6.1 Methodology Overview

Event Tree Analysis (ETA) is typically used for evaluation of systems or processes that have multiple levels of safeguards or safety systems. The ETA methodology helps the analysis team evaluate performance and adequacy of the safety systems, and determine multiple possible consequences for either success or failure of these systems upon demand. The event tree starts from a single initiating event and models the resulting sequence of events.

6.2 ETA Example: Safety Review for Silane Storage and Delivery Room.

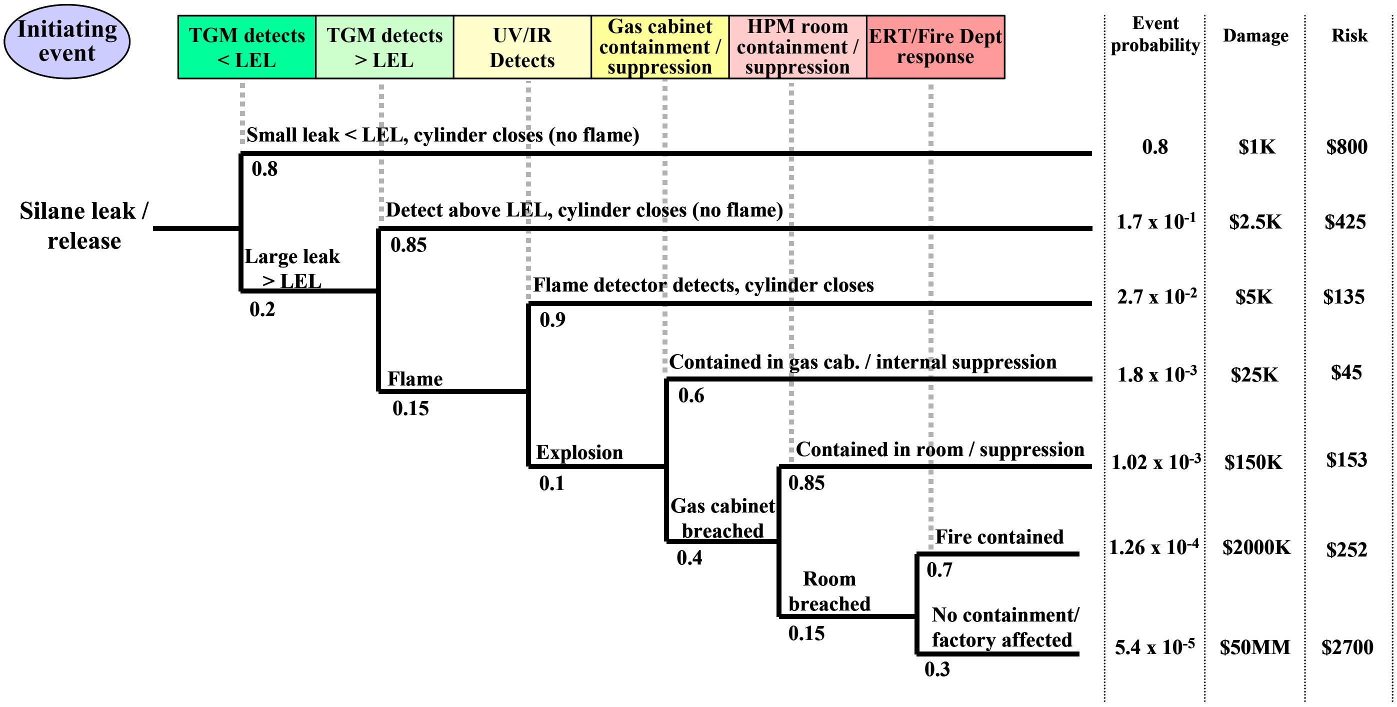
System Description and Lessons Learned

In a typical hazardous materials storage and delivery room, protection systems are engineered and installed to prevent and mitigate hazardous situations such as leaks, fires and toxic exposures. For silane rooms, multiple protective systems are used due to the unpredictable nature of the gas and the potential for delayed or immediate explosions of this pyrophoric gas. In this example, the multiple protective systems for a silane storage and delivery room were evaluated using the Event Tree Analysis methodology. ETA was selected because it was determined (through review of design specifications) that the protective layers were independent and became active as a silane release progressed through a potential leak-fire-explosion cycle. The initial study of the safety systems revealed that there was a relative progression of mitigating systems designed into the silane room. These systems are:

Safeguard systems:

1. TGM detects leak at below LEL and activates cylinder-closing device.
2. TGM detects leak above LEL and activates cylinder-closing device.
3. Decision point – flame or no flame from leak. No flame assumes toxic gas monitoring systems (TGM) fails to detect, therefore a possibility of explosive cloud formation exists.
4. Flame detector senses flame and activates cylinder-closing device.
5. Explosion is contained in gas cabinet.
6. Explosion contained in room, area flame detection / fire suppression activates.
7. Local response team or fire dept. contains external fire before factory is affected.

An event tree was built to model these mitigating systems (Figure 4.1), and success/failure probabilities for each path was stated. These probabilities were estimated from knowledge of system performance of similar systems. Industry average failure rate data for mechanical components was reviewed for applicability, but were not directly used as the primary source of failure / success rate estimates.

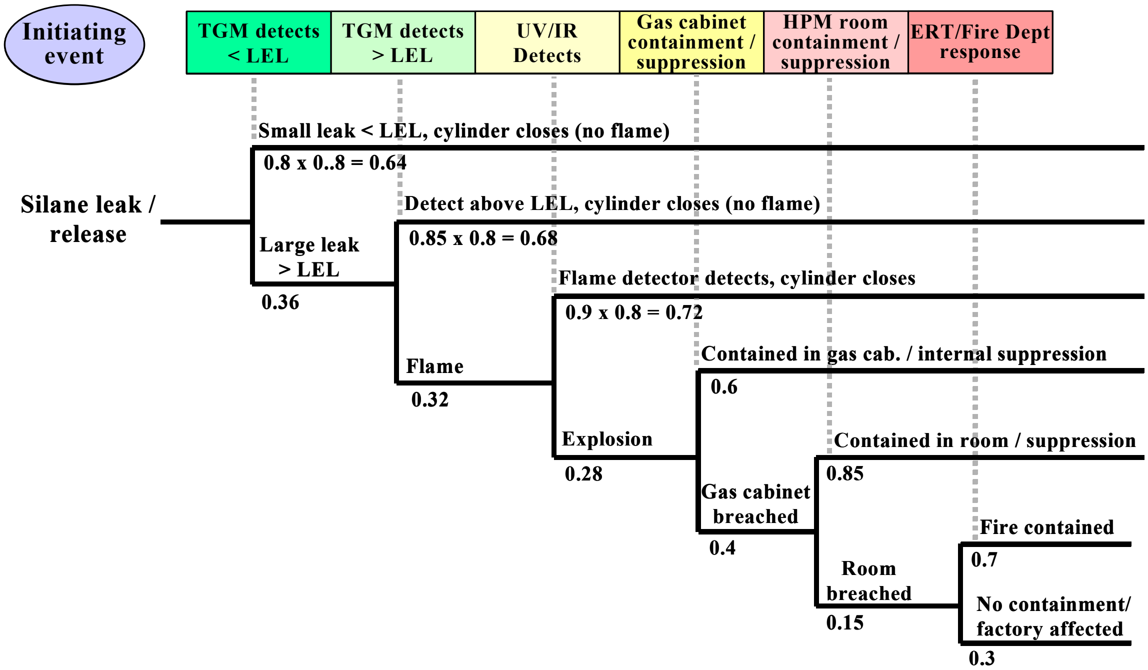

Initiating event
TGM detects < LEL
TGM detects > LEL
UV/IR Detects
Gas cabinet containment / suppression
HPM room containment / suppression
ERT/Fire Dept response
Silane leak / release
Small leak < LEL, cylinder closes (no flame)
0.8
Large leak > LEL
0.2
Detect above LEL, cylinder closes (no flame)
0.85
Flame
0.15
Flame detector detects, cylinder closes
0.9
Explosion
0.1
Contained in gas cab. / internal suppression
0.6
Gas cabinet breached
0.4
Contained in room / suppression
0.85
Room breached
0.15
Fire contained
0.7
No containment/ factory affected
0.3

Event probability	Damage	Risk
0.8	$1K	$800
1.7×10^{-1}	$2.5K	$425
2.7×10^{-2}	$5K	$135
1.8×10^{-3}	$25K	$45
1.02×10^{-3}	$150K	$153
1.26×10^{-4}	$2000K	$252
5.4×10^{-5}	$50MM	$2700

Overall scenario risk: $4510

Figure 6.1: Silane Safety Systems Event Tree

The initial event tree analysis indicated a typical risk characteristic for such systems, i.e. slightly higher adjusted risks for the higher and lower level of controls. However further study of the initial mitigating systems showed a potential common cause component (a mechanically activated automatic cylinder closing device), which had shown historic unreliability as indicated by the site maintenance records (estimated at 20% probability of failure to close on demand). The success probability for the mitigating systems for which this closure device was a part were modified to better represent information gathered from the maintenance data. The event tree was re-quantified using this new probability value, and the results indicated a large increase in overall system risk. (Figure 4.2). Based on this evaluation, it was decided that the mechanical closure device would be replaced with a pneumatically operated closure valve that was integral to the gas cylinder. Cylinder supplier representatives were consulted and confirmed there had been no field failures for these types of pneumatic devices that had been in similar service for over 10 years (the current service life of such devices in the industry at the time of this evaluation).


Initiating event
TGM detects < LEL
TGM detects > LEL
UV/IR Detects
Gas cabinet containment / suppression
HPM room containment / suppression
ERT/Fire Dept response
Silane leak / release
Small leak < LEL, cylinder closes (no flame)
0.8 x 0..8 = 0.64
Large leak > LEL
0.36
Detect above LEL, cylinder closes (no flame)
0.85 x 0.8 = 0.68
Flame
0.32
Flame detector detects, cylinder closes
0.9 x 0.8 = 0.72
Explosion
0.28
Contained in gas cab. / internal suppression
0.6
Gas cabinet breached
0.4
Contained in room / suppression
0.85
Room breached
0.15
Fire contained
0.7
No containment/ factory affected
0.3

Event probability	Damage	Risk
0.64	$1K	$640
2.45 x 10^{-1}	$2.5K	$613
8.3 x 10^{-2}	$5K	$415
1.9 x 10^{-2}	$25K	$475
1.1 x 10^{-2}	$150K	$1650
1.35 x 10^{-3}	$2000K	$2700
5.8 x 10^{-4}	$50MM	$29000

Overall scenario risk: $35,493

Figure 6.2: Silane Safety Systems Event Tree, Modified with Cylinder Closure Probabilities

7. FAULT TREE ANALYSIS (FTA)

7.1 Methodology Overview

Fault Tree Analysis (FTA) is a "top down" assessment methodology which starts with a known or suspected singular system failure event (top event) for which failure scenarios are developed. Singular events or combinations of events are studied to determine how these initiating and contributing elements can propagate to the top event. A fault tree can be quantified to determine the probability of failure for the event of interest, and also can be effectively used as a semi-quantitative or qualitative assessment of relative system risk. A caution should be noted regarding the use of quantitative fault trees. Confidence in a systems' probability of failure rate is dependent upon the quality of failure rate data obtained for the basic events. Unfortunately, most organizations do not have data specific to the equipment they are studying, and therefore must rely on industry average failure rate data. Care should be taken to ensure that this data closely represents the actual equipment and operation conditions of the components within the system being studied, and the analyst (with input from system experts) may need to adjust the failure rate estimates to more adequately represent the equipment and conditions under which it is being operated and maintained.

7.2 FTA Examples

Example 1: Equipment Interlock Removal Study.

A series of manufacturing tools, which utilized toxic chemicals within part of the process, were experiencing periodic unexpected shutdowns. The root cause of these shutdowns was determined to be activation of access panel interlocks, which were tied to the chemical feed valves, and would shut down the supply lines if the interlock circuit was opened. Further investigation uncovered that variations in the internal pressure (created by fluctuations in the exhaust static pressure) caused the access panels to flex, and on occasion would create enough pressure on the interlock switch to decouple the device, resulting in system shutdown. The manufacturing team requested an evaluation to determine if the interlocks could be removed, or if these devices needed to be relocated and/or replaced.

Lessons Learned.
It was decided to utilize the Fault Tree Analysis methodology on this problem, since there was a clear top event of interest (stated as "injury due to chemical exposure") and that a relative risk determination between two options (interlock removal vs. replacement) was needed. A system fault tree was constructed (Figure 3.1) to depict potential failure events and failure combinations, which would result in chemical exposure. Industry average data was used, and a top event failure rate was calculated. The fault tree was then modified (Figure 3.2) by removing the interlock, and a new top event failure rate was calculated. It was observed that the removal of the interlock would increase risk by several orders of magnitude, therefore it was decided that reconfiguration of the interlock system would be the appropriate corrective action. For this equipment, it

was determined that the existing interlocks could be utilized by relocating them to another area of the maintenance panels (near the hinges) where flexing of panel is minimal.

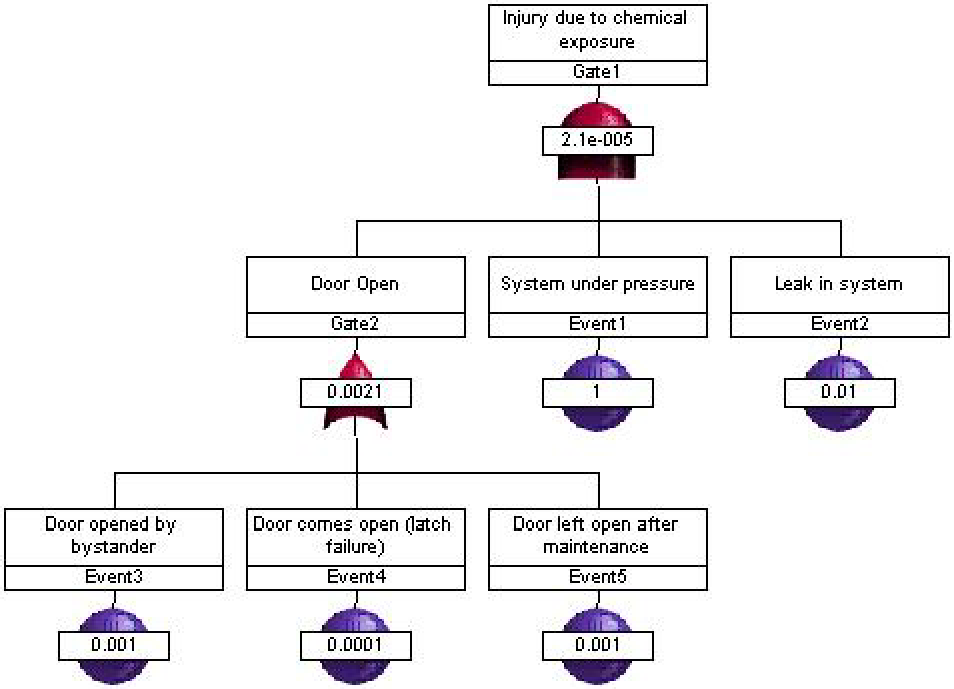


Figure 7.1. Manufacturing Tool Fault Tree, Without Door Interlock Function

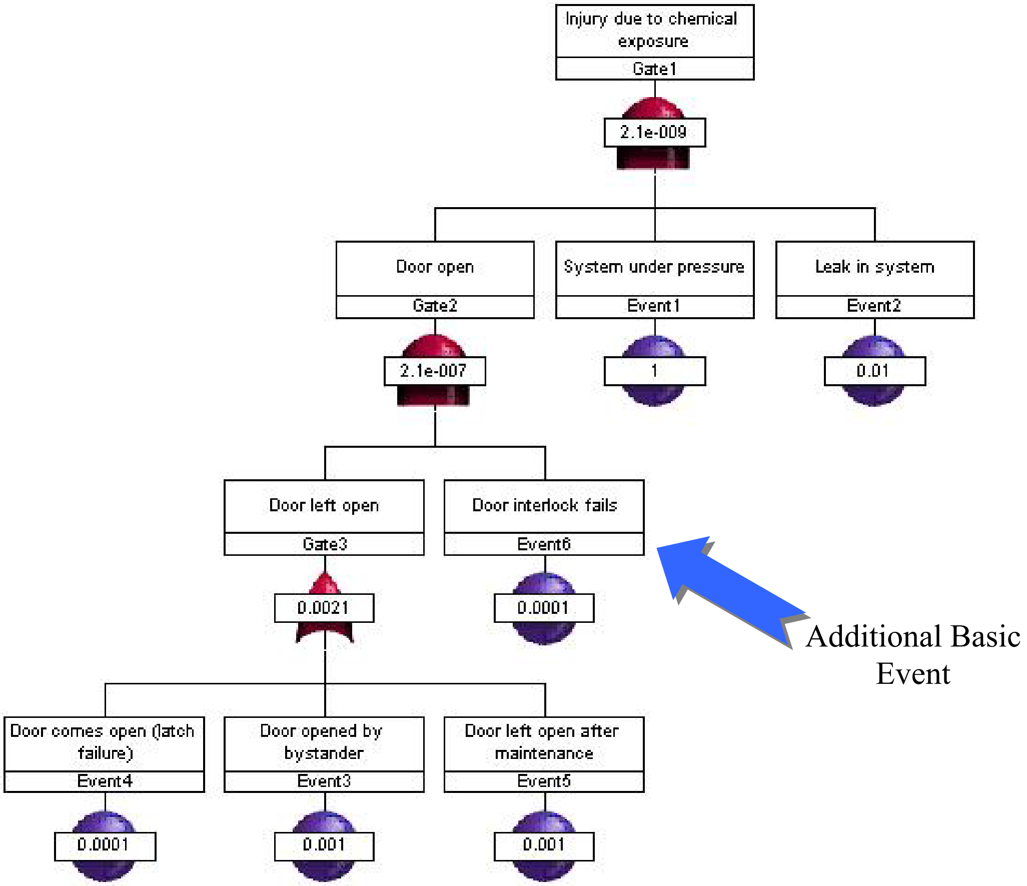


Figure 7.2. Manufacturing Tool Fault Tree, With Door Interlock Function

Level of Effort and Cost to Implement Recommendations.
For this FTA, it is estimated that the lead analyst expended approximately 20 hours conducting data analysis and review, and constructing the fault tree. Additional meetings with system experts and manufacturing personnel to review the results and evaluate the corrective actions took approximately 20 labor hours (total for the team). Relocation of the interlock system was relatively simple and total costs were less than $500 per tool for materials and took 4 labor hours (this included system checkout after relocation).

Example 2: Toxic Gas Cylinder Shutdown Study.

During the Year 2000 shutdown preparations, many of the hazardous process and chemical delivery systems were to be placed in a “safe” standby mode as a precaution in the event facility or utility infrastructure systems were adversely affected. One of the systems being evaluated was the cylinder gas system delivering toxic gases to the factory. It was decided that all the cylinder valves would be shut off, and that all life safety systems (toxic gas monitoring and exhaust systems) would be maintained. Questions were raised about the adequacy of cylinder shutoff, and if additional controls might be necessary.

Lessons Learned.

It was decided to utilize Fault Tree Analysis to evaluate this system, and to determine what dependencies existed among the safety and shutdown features within the system. Industry average reliability data were reviewed and modified (after review by system experts) and when applied, the initial fault tree indicated a low failure rate for the top event of employee exposure. (Figure 3.3).

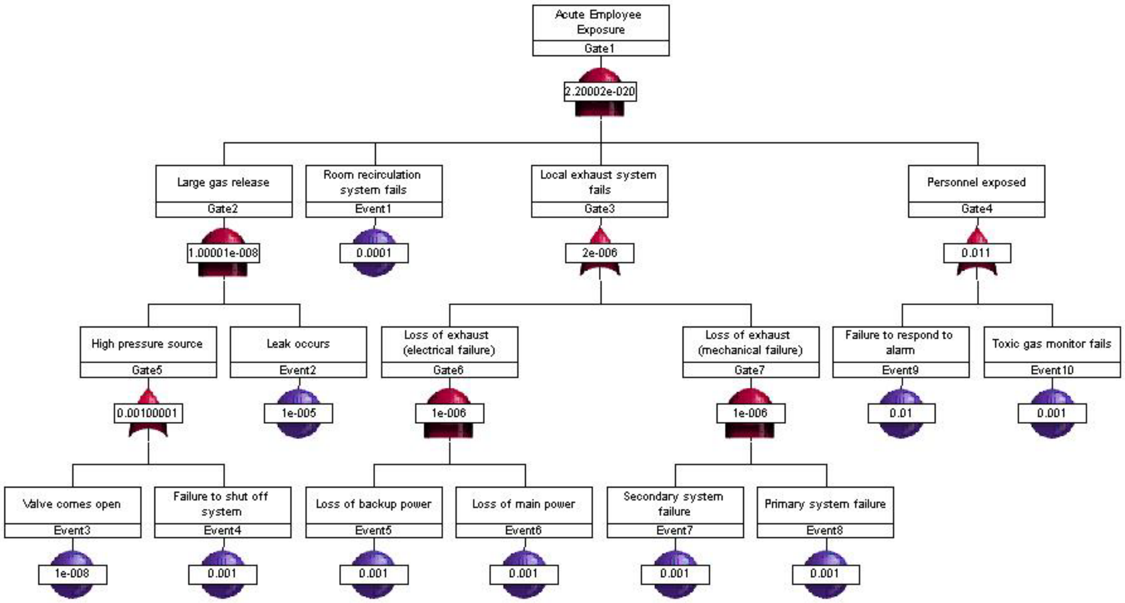


Figure 7.3. Employee Exposure Due to Release from Toxic Gas Cabinet Fault Tree

However upon further review, it was determined that one of the most likely utility failure scenarios for the array of Y2K concerns was loss of power, and that many of the safety systems had direct operational dependency on electricity. (Note, for Y2K many organizations conducted their risk evaluations assuming emergency power would also not be available). When the loss of electricity common cause scenario was considered within the fault tree (Figure 3.4), and the fault tree structure was appropriately modified (Figure 3.5), it indicated an increase in employee exposure risk of many orders of magnitude. At this point, the remaining basic events were studied to determine if or how these systems could be hardened to lower the likelihood of personnel exposure. For 'failure to shut off system' human error event, it was decided that a second, independent verification by another operator would be performed after the cylinder valves had been closed by manual activation of the gas cabinet controller. For the rare event of 'valve comes open', it was decided that the pneumatic control system, which holds the valve open under pressure, would be shut off. Since pneumatic action is the primary means for holding the cylinder open when in operation, the action of depressurizing the pneumatic system will greatly reduce the chance of a valve cylinder opening inadvertently. With these additional controls, the risk of employee exposure was considered acceptable.

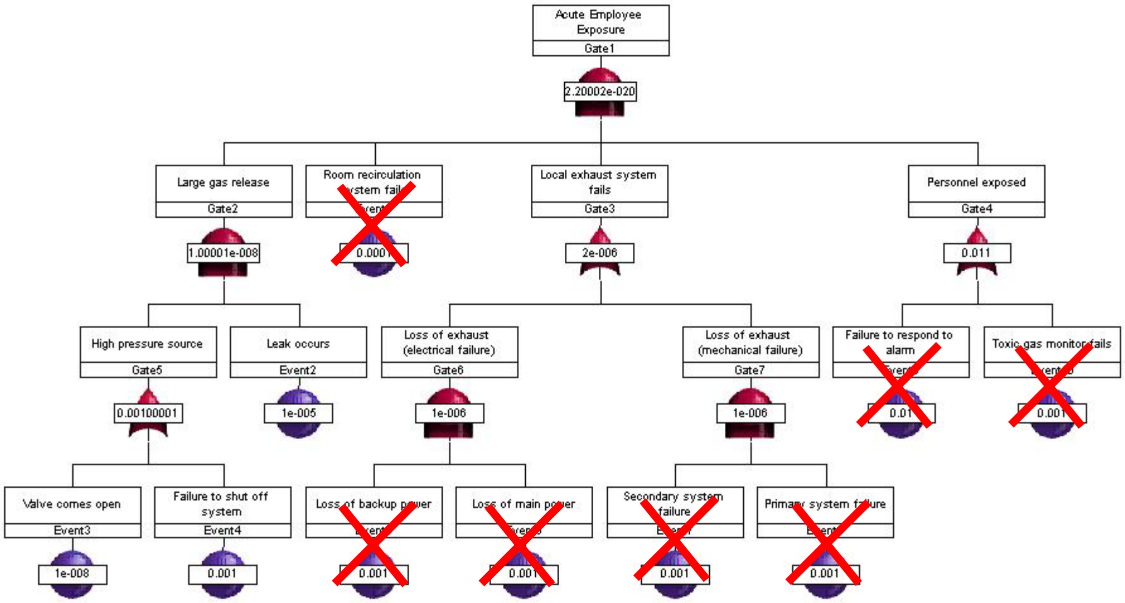


Figure 7.4. Employee Exposure Due to Release from Toxic Gas Cabinet Fault Tree, Effects of Common Cause Power Failure

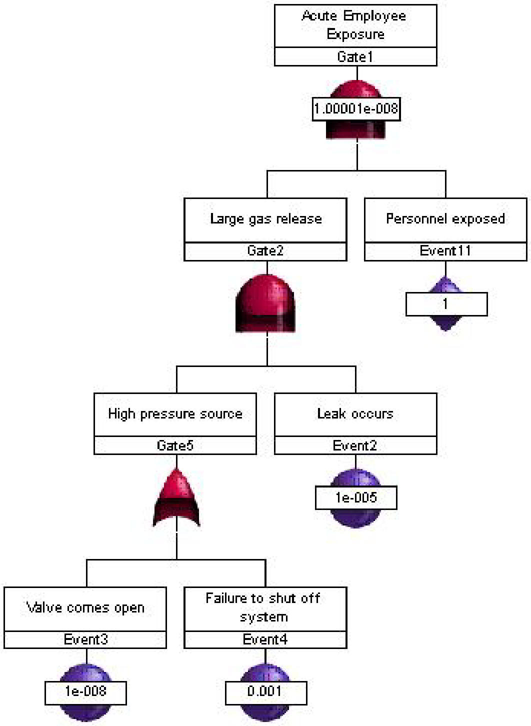


Figure 7.5. Employee Exposure Due to Release from Toxic Gas Cabinet Fault Tree, Catastrophic Power Failure

Level of Effort and Cost to Implement Recommendations.
For this FTA, it is estimated that the lead analyst expended approximately 40 hours conducting data analysis and review, and constructing the fault tree. Additional meetings with system experts and manufacturing personnel to review the results and evaluate the corrective actions took approximately 20 labor hours (total for the team). There were no material costs associated with the recommendations, and it was estimated that only 4 additional labor hours would be expended to conduct the independent verification of cylinder valve closure.

8. SAFETY ANALYSIS REVIEW (SAR)

8.1 Methodology Overview

SAR involves detailed inspections/reviews to identify process or facility conditions, operating practices or maintenance activities that could cause an accident. DoE Order 5481.1B gives general guidelines and preferred practices for organizations engaged in the review and documentation of facility safety operations. These guidelines require: Facility description; system design criteria; components and structures; normal and emergency operating procedures; identification of hazards, potential accidents, probability of occurrence, and predicted consequences of hazards; physical design features; and administrative controls to prevent or mitigate potential accidents and operational limitations. During a SAR, a team would examine the site, building and individual laboratories to assess if they comply with applicable codes and regulations (e.g., OSHA, EPA, DOT, UFC, UBC, NFPA and internal codes). They will compile a list of potential accident initiating events, following a brainstorming technique such as "what if" or a more structured one, such as HazOp. A level of probability and consequence is assigned to each accident scenario, based on industry generic or internal data, and the risk associated with each scenario is estimated as the product of probability and consequence. The primary role of SAR is to identify relatively high risk accident-initiating scenarios and determine if sufficient layers of protection exist to safeguard against such scenarios.

8.2 Example: SAR of NREL Bldg. 16

A safety self-appraisal audit at NREL, Golden, CO, identified a number of discrepancies that could affect safety in a building with mixed laboratory and office occupancy. Several hazardous materials were used in the laboratories (Table 8.1) in quantities that could cause harm and some deficiencies in safety systems and procedures were identified. A team of facility and outside EHS experts worked together inspecting all laboratory systems, codes and protocols and they identified several potential accident-initiating scenarios, their expected frequency, and associated consequences (Table 2). Then a relative risk matrix was used to assess the remaining scenarios. Risk was determined as the product of probability and consequences by using order of magnitude data. The matrix of probability and consequence in Table 3 gives semi-quantitative measures of risk in four classes: routine, low, moderate, and high. The risk is defined in relative terms with the objective to identify relatively high risks and eliminate them. Early on it was decided to move the 100% silane operations in another building with open-storage and dedicated controls. Of the remaining 30 potential accident-initiating events identified by the team, none present high or moderate risks, and 21 present low risks (Table 2). Let us describe how the first scenario in Table 3, "leak in a pyrophoric gas distribution system into gas cabinet or system enclosure" was assessed to be of low risk. The probability was assessed to be remote based on the probabilities of piping failures (10^{-6} faults/yr), gasket leaks (0.01 faults/yr) and the fact that no such initiating events have occurred in the lifetime of NREL's CVD systems (four systems an average life cycle of four years). To determine the potential consequences, the flow through an open valve and the concentration build-up in the cabinet or enclosure was calculated.

The resulting concentrations under the assumptions of unmitigated scenario were then compared with the IDLH concentration and with the minimum flammability limits of the gas. Finally the control systems in place were assessed. These included flow restricting and excess flow valves, auto-shut down on the cylinder, exhaust ducts composed of fire-resistant materials and fire-suppression systems. The consequence level was assessed to be marginal, potentially causing damage in the range of $10,000 to $100,000.

Table 8.1. Typical HPMs used to produce photovoltaic devices

HPM	**Type of hazard(s)**
Arsine	Highly toxic gas
Phosphine	Highly toxic and phyrophoric gas
Hydrogen selenide	Highly toxic
Tungsten hexafluoride	Toxic and corrosive gas
Molybdenum hexafluoride	Toxic and corrosive gas
Silicon tetrafluoride	Toxic and corrosive gas
Tertiarybutylarsine	Pyrophoric and highly toxic liquid
Tertiarybutylphosphine	Pyrophoric liquid
Trimethylgallium	Pyrophoric liquid
Trimethylaluminum	Pyrophoric liquid
Diethylzinc	Pyrophoric liquid
Trimethylindium	Pyrophoric solid
Diethylsilane	Flammable liquid
Lightly doped mixtures	Flammable gas
Hydrogen	Flammable gas
Methane	Flammable gas
Hydrogen chloride	Corrosive gas
Oxygen	Gaseous oxidizer
1% silane in helium	Compressed gas

Table 8.2. Risk Analysis Results

	Probability						Consequence				Risk			
Transient description	**I**	**ER**	**R**	**O**	**RP**	**F**	**N**	**M**	**C**	**CA**	**R**	**L**	**M**	**H**
Leak in pyrophoric gas distribution system into gas cabinet or system enclosure			*					*				*		
Quantity in excess of B-2 occupancy ordered				*			*				*			
Leak in cylinder			*						*			*		
Intralaboratory transportation accident		*						*			*			
Cross-threading of valve compressed gas association fitting and failure of helium leak check		*						*			*			
Missing washer in HCI or H_2Se cylinder			*					*			*			
Forgetting washer/gasket in a gasketed gas connection			*						*			*		
Attempt to open sticky cylinder cap using a wrench as a lever			*						*			*		
Toxic/pyrophoric liquid bubbler put in backwards			*				*				*			
Toxic/pyrophoric liquid bubbler leak outside delivery system				*				*				*		
Leak of air in vacuum pump			*					*				*		
Leak in toxic gas distribution system into gas cabinet or system enclosure			*						*			*		
Leak in distribution system between gas cabinet and deposition system and failure of secondary containment (coaxial tubing or ducting raceway)		*							*			*		
Faulty seals connecting reactor vessel to system				*				*				*		
Rupture of quartz reactor vessel			*					*				*		
Hydrogen leak in gas cabinet			*						*			*		
Hydrogen leak in purifier			*					*				*		
Loss of process control with potential for episodic release of AsH_3, PH_3, and/or H_2Se			*					*				*		
Loss of process control and simultaneous failure of scram unit, exhaust scrubber, or cylinder valve		*						*			*			
Loss of exhaust, ventilation					*		*				*			
Liquid-type effluent scrubber blockage					*		*				*			
Excessive oxygen in carbon drum effluent scrubber and buildup of unreacted hydrides and/or metal-organics			*						*			*		
Effluent removal fails due to loss of system vacuum				*			*				*			
Burn box (combustion, decomposition, and oxidation) flame goes out				*			*				*			
Loss of containment of carbon drum contents			*					*				*		
Operator exposed to toxic by-product materials			*				*				*			
Caustic spill of sodium hydroxide disposal (pH 13.8)				*				*				*		
Fire			*					*				*		
Seismic activity			*						*			*		
High winds and tornadoes			*				*				*			
Totals	**0**	**4**	**18**	**6**	**2**	**0**	**8**	**14**	**8**	**0**	**12**	**18**	**0**	**0**

Key

Probability		Consequence	Risk
I: Impossible	**RP:** Reasonably probable	**N:** Negligible	**R:** Routine
O: Occasional	**R:** Remote	**M:** Marginal	**L:** Low
ER: Extremely remote	**F:** Frequent	**C:** Critical	**M:** Moderate
		CA: Catastrophic	**H:** High

Table 8.3. Risk Assessment Matrix

	PROBABILITY					
CONSEQUENCE	A Frequent	B Reasonably Probable	C Occasional	D Remote	E Extremely Remote	F Impossible
I Catastrophic	🟥 HIGH	🟥 RISK	🟥	🟪	🟨	🟩
II Critical	🟥	🟥	🟪 LOW	🟨	🟨	🟩
III Marginal	🟪	🟪	🟨	🟨 MODERATE	🟩	🟩
IV Negligible	🟩	🟩	🟩	🟩	🟩	🟩 ROUTINE

Event Probability Classification

Frequent (>1.0). Likely to occur many times during the life cycle of the system (test/activity/operation).

Reasonably probably (0.1-1.0). Likely to occur some time during the life cycle of the system.

Occasional (0.01-0.1). Likely to occur some time during the life cycle of the system.

Remote (10^{-4}-10^{-2}). Not likely to occur in the life cycle of the system, but possible.

Extremely remote (10^{-6}-10^{-4}). Probability of occurrence cannot be distinguished from zero.

Impossible (<10^{-6}). Physically impossible to occur.

Hazard Consequence Classification

Catastrophic (loss >$1 million). May cause death or system loss.

Critical ($100,000-$1 million). May cause severe injury or occupational illness or minor system damage.

Marginal ($10,000-$100,000). May cause minor injury, occupation illness, or system damage.

Negligible (<$10,000). Will not result in injury, occupational illness, or system damage.

Risk Category

Routine:Risk no different from those experienced by any individual in his or her daily life.

Low risk:Events may have impact within a facility but little or no impact to adjacent facilities, public health, or the environment.

Moderate risk:Events have potential impacts within the facility but at most only minor impacts off site.

High risk:Events have the potential for on-site and off-site impacts to large numbers of persons or major impacts to the environment.

9. LAYERS OF PROTECTION ANALYSIS (LOPA)

9.1 Methodology Overview

Layer of Protection Analysis (LOPA) is generally not utilized as a stand-alone analysis methodology. It is best applied as a further review of protective layers based on failure scenarios developed from initial qualitative hazard analysis studies. Unlike Fault Tree and Event Tree Analyses which can be quantified to determine system probability of failure, LOPA uses orders of magnitude approximations for estimating initiating event frequency, severity of the consequence and the likelihood of failure of the independent protection layers (IPLs). The concepts of LOPA are to (1) identify those detections (protections) that are truly independent of the cause and each other, and (2) score those independent protection layers (IPLs) via a simple, standardized scale. This separate assessment of the detection for selected cause-consequence pairs helps ensure that the team does not overlook critical weaknesses and underestimate the reliability of controls.

In the following example, an arithmetic calculation method was used to judge adequacy of identified or applied controls. This method uses the basic equation:
$\text{Frequency}_{\text{Consequence}} = \text{Frequency}_{\text{Initiating Event}} \times U_i$; where U_i is the product of the probability of failure on demand (PFOD) for the independent protection layers.

The values estimated for IPLs, consequence and initiating event frequencies were determined by the analysis team, using published estimates,which were modified or validated by the team. Where possible, internal historical information (mostly empirical data) was used to establish the values used in this example. Caution should be exercised when using estimates published by external entities (including those in this example), as they may not adequately represent scenarios developed for other operations.

9.2 Example: Bulk Silane Installation Hazards Analysis

Outdoor installations of bulk silane has long been debated as a potentially safer method of delivering this pyrophoric gas. In addition to the potential for enhancing facility and personnel safety, significant cost savings can be realized via bulk purchase of this process gas. Due to the quantity of hazardous materials associated with the bulk installation, there is great interest by management, local authorities and the general public to ensure that appropriate protective systems are in place and are sufficiently reliable to prevent or mitigate a gas release. In this example, an initial hazards analysis (HazOp) was performed on the bulk installation system which identified potential release scenarios and associated controls. It was decided that additional review of these controls and other protective schemes was desired to fully understand their effectiveness for the larger release scenarios. LOPA was chosen since it is effective for reviewing systems on which multiple layers of controls (independent protective layers) are applied.

A layout of the bulk silane delivery system is shown in Figure 9.1.

From the HazOp study, the significant release scenarios and associated control features were identified as shown in Table 9.1.

Table 9.1. Significant Release Scenarios from HazOp Study

Failure/Deviation	Cause	Existing Controls
Large silane release from tube trailer.	External wildfire impinges on tube trailer.	Fire break around delivery pad.
Large silane release from tube trailer.	Flame impingement from adjacent tube trailer or back-up vessel.	UV/IR sensor tied to deluge system.
Large silane release from a piping break.	Impact to delivery line from equipment operating in the area.	Pipe routed in remote area, except for pipe bridges over two access roads.

Estimates for consequence frequency can be derived from other analytical studies or from industry information. In this example, frequencies of significant silane releases were derived from a separate Fault Tree Analysis, and are shown in Table 9.2.

Table 9.2. Significant Incident Frequency, Bulk Silane System

Silane Release, Bulk Delivery System	
Large release from tube, tube failure. [1]	1.6×10^{-5}
Tube trailer release and fireball / flame. [2]	3.4×10^{-5}
Large release from piping system break, equipment related.	5×10^{-5}
Large release from piping system break, external impact / affect.	1×10^{-4}
[1] release and accumulation with explosion potential [2] external event or component failure with immediate ignition	

A standardized table is used to pick initiating event frequencies which are applicable to the system being studied. Table 9.3, derived from industry information and estimates based on internal company data were used.

Table 9.3. Initiating Event Frequencies

Initiating Events (Equipment)	Typical Frequency	
Vessel failure (manufacturing defect)	1 / 1000 yr.	10^{-3}
Vessel failure (out-of-spec process conditions)	1 / 100 yr.	10^{-2}
Piping or component failure (manufacturing defect)	1 / 100 yr.	10^{-2}
Piping or component failure (out-of-spec conditions)	1 / 10 yr.	10^{-1}
Vessel or piping failures due to extreme environmental conditions	1 / 100 yr.	10^{-2}
Vessel or piping failure due to wear-out	1 / 10 yr.	10^{-1}
Initiating Events (Human Error)		
Vessel failures (external impact)	1 / 10 yr.	10^{-1}
Piping failures (external impact)	1 / 10 yr.	10^{-1}
Operational Human Error		
- once per day opportunity	1 / yr.	10^{0}
- once per month opportunity	1 / 10 yr.	10^{-1}
- non-routine operation	1 / 10 yr.	10^{-1}

Independent Level of Protection probability of failure on demand (PFOD) values, determined from industry average tables and internally derived estimations were established and shown in Table 9.4.

Table 9.4. Independent Protection Layer PFOD

Human Intervention	PFOD
Manual response in field when > 10 minutes available for response.	10^{-1}
Manual response in field when > 40 minutes available for response.	10^{-2}
Manual response to abnormal input with immediate diagnostics aid.	10^{-2}
Manual response to abnormal input without a diagnostics aid.	10^{-1}
Passive Devices	
Secondary containment or barriers requiring periodic maintenance (e.g. earthen berms).	10^{-2}
Secondary containment or barriers requiring periodic inspection (e.g. concrete berms, walls).	10^{-4}
Passive transfer devices requiring periodic inspection (e.g. overflow pipes and weirs)	10^{-2}
Active Devices*	
Automatic sprinkler system	10^{-1}
Automatic deluge system	10^{-2}
Fire detection systems (UV/IR)	10^{-2}
Standard smoke detection systems	10^{-1}
Early warning smoke detection system	10^{-2}
* activation components and controls may need independent review and analysis	

Revisiting the three high-consequence failure scenarios from the HazOp study, the values from the table can be applied to determine if adequate protection layers are in place.

For the first scenario:

Failure/Deviation	Cause	Existing Controls
Large silane release from tube trailer.	External wildfire impinges on tube trailer.	Fire break around delivery pad.

The equation Fi = Fc x Ui is solved as $10^{-5} > 10^{-2} \times 10^{-2}$. Since Fc x Ui is still greater than Fi, it is recommended that additional controls be investigated. In this case, we can extend the UV/IR detection (to activate a deluge system) in the vicinity of the silane tube trailer, including the fire break area around the perimeter of the pad. As shown in the tables, UV/IR systems would affect the equation: $10^{-5} < 10^{-2} \times (10^{-2} \times 10^{-2})$. Now Fc x Ui is smaller than Fi, and it is judged that adequate protective layers exist.

For the second scenario:

Failure/Deviation	Cause	Existing Controls
Large silane release from tube trailer.	Flame impingement from adjacent tube trailer or back-up vessel.	UV/IR sensor tied to deluge system.

The equation Fi = Fc x Ui is solved as $10^{-5} > 10^{-2} \times 10^{-2}$. Since Fc x Ui is still greater than Fi, it is recommended that additional controls be investigated. In this case, we can erect an additional physical barrier (concrete wall) to protect the adjacent equipment from fire impingement. As shown in the tables, concrete type barrier wall systems would affect the equation: $10^{-5} < 10^{-2} \times (10^{-2} \times 10^{-4})$. Now Fc x Ui is much smaller than Fi, and it is judged that adequate protective layers exist.

For the third scenario:

Failure/Deviation	Cause	Existing Controls
Large silane release from a piping break.	Impact to delivery line from equipment operating in the area.	Pipe routed in remote area, except for pipe bridges over two access roads.

The equation Fi = Fc x Ui is solved as $10^{-4} > 10^{-1} \times 10^{-0}$. Since Fc x Ui is still greater than Fi, it is recommended that additional controls be investigated. In this case, we can erect an additional physical barriers around and on the overhead pipe bridges to protect against impact damage. As shown in the tables, such substantial passive barriers requiring periodic inspection, would affect the equation: $10^{-4} < 10^{-1} \times (10^{0} \times 10^{-4})$. Now Fc x Ui is smaller than Fi, and it is judged that adequate protective layers exist.

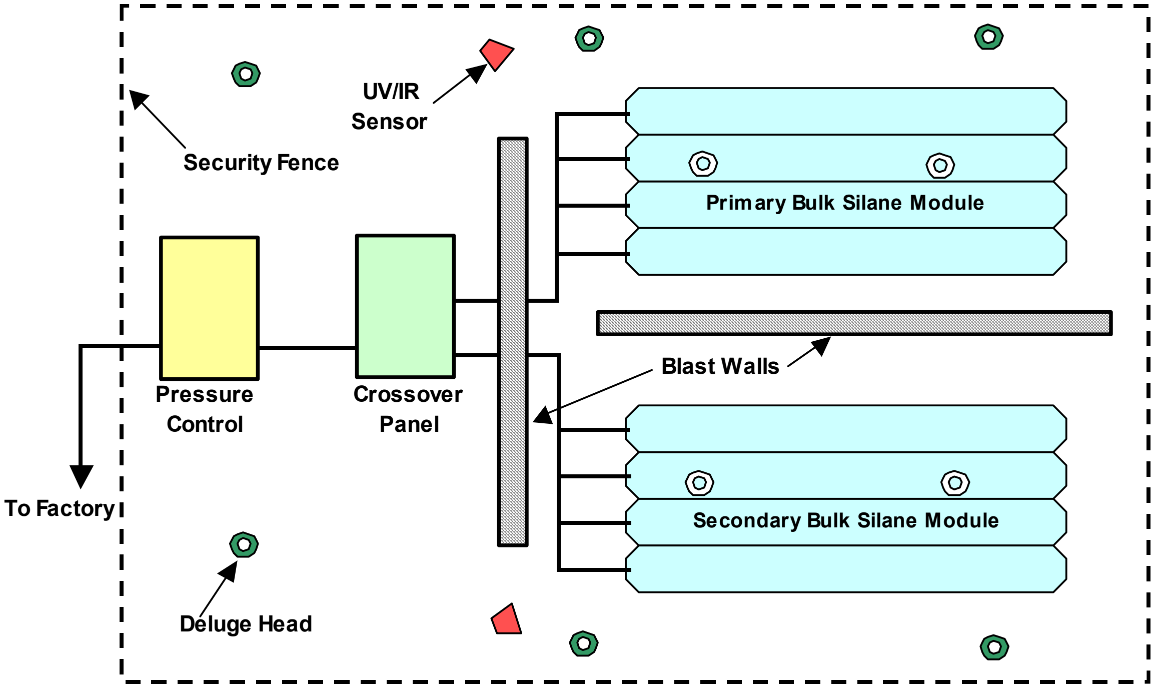


Figure 9.1. Bulk Silane Delivery System Equipment Layout

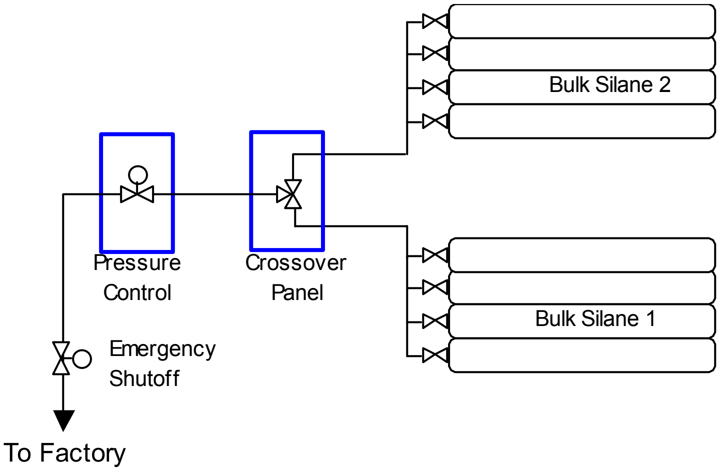


Figure 9.2. Bulk Silane System PID

10. SECURITY RISK ANALYSIS

Security Risk Analysis as presented in this report, is a relative risk assessment that can augment conventional process hazard analysis. This assessment is based on categorizing threat, vulnerability, and the consequences of deliberate actions by terrorists, disgruntled employees, and others. The consequences of releasing hazardous materials to the environment are the same regardless of whether the release results from equipment failure, an accident, natural causes, or malevolent action. Like accidental releases, the risk associated with adversarial action can be mitigated through a protection system that combines engineering, administrative, and personal controls. Engineering measures that would prevent accidents or reduce the consequences of environmental release may be equally applicable in considering adversarial actions. In addition to health and environmental consequences, the loss of production capacity is an outcome of hostile action that may be unacceptable to a chemical producer. Table 10.1 is a generic checklist for the physical-security planning process. Additional checklists are given for planning, and implementing, a security system for a chemical-production facility or for a research and development (R& laboratory are shown in Tables 10.2 and 10.3.

The elements of this analysis are discussed below (these are extracted from a paper by Lemley, Fthenakis and Moskowitz, published in Process Safety Progress, September 2003).

10.1 Identification of the Target

The first step in the planning process is to determine and document what needs to be protected. These are the features of a facility and items contained therein that are attractive to presumed adversaries, and/or involve risk that would be unacceptable without adequate protection. Although a chemical facility contains many potentially vulnerable targets for some type of threat, this analysis addresses primarily those unique targets for which a safety analysis identified significant adverse consequences of accidental release. Other types of targets, such as property protection areas, are discussed briefly to illustrate the principles of protection-program planning and the objectives of the physical security system.

Table 10.1. Generic Security Planning Analysis

1. Describe what is to be protected.

2. Define the consequences, for example, of theft, sabotage, compromise of information, fire, natural disaster, unauthorized access.

3. Define the adversaries, for example, criminals, disgruntled employees/customers, mentally unstable individuals, vandals, terrorists, violent activists, [all may include insiders] natural phenomena, and equipment malfunctions.

4. List the vulnerabilities, such as unsecured facility, public access, faulty access controls, unaccounted-for keys, ground-level windows, no security/fire alarms, no circulation controls [badges], and flood-prone area).

5. Plan, fund, and implement corrective actions. Examples are Security alarms, cameras [recordable], fire alarms, locks and key control procedures, employee access- and circulation-controls, visitor-control procedures, back-up power, and communications plans to alert authorities.

6. Describe the security procedures in place after the upgrades.

7. Define the responses to the mitigated threats to establish an acceptable risk.

8. Test and validate the responses; establish the frequency of testing.

9. Review the plan annually and update as necessary.

10.2 Threat Definition

The threats from which the assets (targets) at a chemical facility need to be protected must be identified and documented in the facility's security plan, and must consider both outsider- and insider-threats. An outsider is an adversary who does not have routine access to the facility. An insider has such routine access, but possibly not to the area containing a particular target. Each facility should prepare a list of threats to serve its own requirements for security planning. The Department of Energy (DOE) issued generic threat guidance for their facilities that are vital to national security. In the following paragraphs, we present an unclassified categorization derived from this classified guidance, identifying threat groups that may require attention in planning a protection program.

Terrorists. Since September 11, 2001, terrorism is seen as a much more likely threat. The probability of this threat may depend greatly on the facility’s location, and on its relative attractiveness compared to other types of facilities nearby. Federal and local law-enforcement agencies may help in evaluating the terrorist threat in a particular area. Federal ownership is believed to increase the attractiveness of a facility for terrorist activity relative to neighboring facilities. Unless the terrorist is a suicidal "martyr", the probability of escaping is of major importance. Thus, a non-suicidal terrorist might choose to attack a less well-protected facility.

Criminals. The security risk from criminals is theft of property, information or services.

Psychotics. Psychotics are mentally ill persons who are out of touch with reality. Equipped with weapons or explosives, they could present considerable risk. The psychotic may not be deterred by the possibility of being caught or injured.

Disgruntled employee. A disgruntled employee is a type of insider threat. An insider has routine access to parts of the facility, and may have major knowledge about the facility's protective systems. A disgruntled employee might want to inflict damage on a chemical-production facility by releasing HPMs or by destroying its production capacity.

Violent activists. This assailant has weapons or explosives and is prepared to use them in attacking a facility.

Intelligence collectors. This adversary could be an insider or an outsider attempting to steal proprietary information at a high-tech facility.

Militia/Paramilitary. These groups may include hostile insiders and outsiders. Facility management should consult with local law-enforcement agencies (LLEA) to determine if this type of enemy is active in the area and likely to be a threat to the facility.

Insiders. Insiders may act alone or participate with any of the threat groups described above. Insiders' motivation may vary considerably. It may be passive non-violent, (i.e., the insider provides information about the facility to others), but has no active role in the threat scenario. Insiders may actively participate in the threat scenario in either a non-violent or violent manner.

10.3 Threat Guidance

Guidance on threats should document the combinations of types of threat, the motivations of the various members of the threat-group, and their likely equipment (e.g., firearms, explosives, and break-in tools) that must be considered in planning or evaluating security for a facility. This guidance may be provided by oversight agencies. A facility should develop its own specific threat guidance by adapting such governmental guidance and by working with local law enforcement agencies and local branches of federal law enforcement and intelligence agencies. Any facility should carefully control the dissemination of its threat-guidance documents and other information about its protective systems that might be useful to an adversary planning to attack the facility.

10.4 Risk

Risk is defined as a combination of three factors: the likelihood of a threat (adversarial action); the vulnerability of a facility or the target of the threat (related to the probability that an attempted enemy action would be successful); and, the probable consequences should an adversarial action be successful. The vulnerability and the consequences might possibly be quantified; however the probability of a particular threat is impossible to estimate. Fortunately, calculating the absolute risk is not necessary if an accurate relative ranking of risk can be obtained. The following methodology can be used to quantify such relative risk.

Risk is represented as the product of the potential threat, the facility's or system's vulnerability to malevolent acts that may be attempted by the various adversarial groups, and the consequences that may occur if the malevolent event is successful.

Risk = Threat x Vulnerability x Consequences

A set of threats is identified, a set of possible targets with specific vulnerabilities is developed, and the consequences are specified for each target if the threat were to succeed. The particular or absolute value assigned to these parameters is not important; rather the *relative* ranking is important and must be done consistently. Relative risk is seen as a systematic and more appropriate measure than estimates obtained by considering only one element of risk, for example, vulnerability. The design or upgrading of security systems should not be driven by vulnerabilities alone (nor by threats or consequences), as has often been the case. From a cost-effective viewpoint, not every potential vulnerability must be corrected since the consequences associated with a particular vulnerability may be minimal.

10.5 Consequences

The release of HPMs could injure facility personnel and the general public, and cause a temporary, or possibly permanent, loss of production. Damage to production equipment also would interrupt production. The security system must address scenarios with these consequences of hostile actions. Safety systems are installed to mitigate the consequences of accidental release of HPMs. These same vital systems also would lessen the effects of a release through other means provided that their critical components are protected. Two types of consequences of adversarial action at a chemical facility are considered in this security planning and evaluation methodology. 1) The release of HPMs that can injure or kill facility personnel or members of the general public, and/or degrade the environment. 2) Damage to expensive and/or unique production equipment that would be costly to repair or replace, and that would disrupt production capability with the concomitant loss of revenue.

These are essentially the same consequences as those identified in safety-analysis reports for chemical facilities as the outcome of accidents or equipment failure. Further, the same categorization of consequence levels developed for safety analyses is applicable to the consequences from attacks at a process facility.

10.6 Vulnerability

Vulnerability is the likelihood that a particular threat scenario would succeed if it were attempted. Ranking of the vulnerability of facility targets to various threats is based on understanding of the effectiveness of the facility's protective systems. In ranking vulnerability, the absolute values are not important; it is only necessary to generate correct, consistent relative rankings.

Protective systems can be employed to reduce vulnerability. At a chemical-process facility, they may be installed to reduce the susceptibility of areas where HPMs are stored or used. Examples of such protective-system components include fences, vehicle access barriers, alarm systems, video assessment systems, communication systems, and response forces. In planning protective systems, or modifying them, the most cost-effective approach is to focus on reducing the overall risk rather than just the vulnerability component.

10.7 Ranking Levels

Threat Categorization Level

Considering the location of the facility and using information from the LLEA and the history of the process facility itself may be useful in assigning relative ranks to threats according to the following definitions:

L = Low. Not likely to threaten. Adversary is not present in geographic area or not active. Few, if any, incidents or attempts have occurred, and none recently.

M = Medium. Possibility of a malevolent operation. Incidents have occurred or been attempted at the facility, or in the immediate geographical area.

H = High. Strong possibility of malevolent action over time. Frequent or serious incidents have occurred or been attempted at the facility or in the immediate geographic area.

Vulnerability Categorization Level

Vulnerability assessment tools developed by the DOE's contractors can be used to analyze and rank a facility's vulnerabilities. A qualitative ranking usually can be made by those familiar with the protective systems, and may be validated by performance tests and from performance data for systems with comparable components. The following definitions may be useful in establishing valid relative rankings of vulnerability level.

L = Low. No readily exploitable vulnerabilities apparent. An adversary would require extensive effort and/or time to complete a successful attack.

M = Medium. Existing vulnerabilities may cause operational degradation if they were successfully exploited. An adversary would have to plan the attack to thwart the protective measures. The enemy may encounter defensive measures before completing the malevolent act.

H = High. Major vulnerabilities exist that are not entirely mitigated by protection measures. An adversary could exploit these vulnerabilities before detection is effective and intervention likely.

Consequence Categorization Level

The consequences of an attack can be characterized for several elements. One element would be the health and safety of workers and the general public. A second would be the possible monetary costs of recovery including repairing damage to the physical plant, cleanup, and restoring the environment. A third element would be the possible impact on programs or production, including possible shutdown of the plant and loss of production while completing corrective actions and environmental cleanup. Another possible consequential element is harm to national security.

Since the consequences of release of HPMs are essentially the same, regardless of whether they are due to an accident, equipment failure, or malevolent act, the relative confidence levels developed for safety analyses can be used in evaluating a facility's security system. We use the same four-level consequence classification as the one we used in the SAR section.

N = Negligible (loss, cleanup costs <$10,000). These will not result in injury, occupational illness, or system damage; the cleanup and environmental- restoration costs are negligible.

M = Marginal (loss, cleanup costs $10,000-$100,000). These may cause minor injury, occupational illness, or system damage; there are some costs for cleanup and environmental restoration.

C = Critical (loss, cleanup costs $100,000-$1 million). These may cause severe injury or occupational illness; the costs for cleanup and environmental restoration are significant.

K = Catastrophic (loss, cleanup costs >$1 million). These may cause death or system loss, shutdown of the plant and associated severe economic loss, and major expenses for cleanup and environmental restoration.

10.8 Evaluating Risk

Similarly to SAR and LOPA, we assign approximate numerical values to the levels defined above for each of the risk elements. In human-factors research, people group items or sense significant differences when levels change by multiplicative factors. They group likelihood more by logarithmic differences than by arithmetic ones. Using that principle here, the multiplicative factor that moves a Low to Medium is the same factor that will change a Medium to High. Recent risk assessment work at Brookhaven suggested that the total range from low to high for threat likelihood is only about a factor of 10. Therefore, using the multiplicative rule, the following values are assigned to the level of threat likelihood: Low=1, Medium=square root of 10 (=3.2), High=10. These values should be modified if, for example, local information suggests that a more extreme range of threats would be realistic and meaningful, or if more than three levels of threat likelihood can be meaningfully distinguished.

Similarly for vulnerabilities, Brookhaven judged, from its knowledge of and experience with security systems, that the total range of vulnerability from Low to High was only about a factor of 10. Again, from experience and using the multiplicative rule, the following values are assigned to the levels of vulnerability: Low=1, Medium=square root of 10 (=3.2), High=10.

It is postulated that the consequences of the release of HPMs through malevolent acts would be similar to those caused by accidents or equipment failure. In both cases, the consequences that must be considered are personal injury, death, and environmental contamination. From the security viewpoint, the loss of facility assets, including the production equipment must be carefully thought about. Such losses could result from direct physical damage, or contamination due to release of HPMs. Also, the expenses of environmental cleanup and remediation must be included. Furthermore, since the facility might become inoperable or have to be closed, the programmatic impact and loss of production, especially for commercial facilities, should be weighed in.

The relative severity of these consequences can be ranked in terms of dollar costs. Logarithmic differences in costs are meaningful in evaluating the impact of losses and the cost-effectiveness of systems for prevention, mitigation, remediation, and recovery. These levels are Negligible<$\$10^4$; Marginal $\$10^4$-$\$10^5$; Critical $\$10^5$-$\$10^6$; and, Catastrophic >$1 million.

For risk assessment purposes, the range of consequences could be extended to distinguish from the others those consequences with cost impacts in the range of tens of millions of dollars, or the value of the entire facility. If the upshot of a security incident was the permanent closure of the entire facility or for an extended time, the range of consequences should cover the value of the entire facility, including the site and/or the value of production during the non-productive period. It also should be determined whether the costs of cleanup and environmental remediation might exceed the value of the entire facility. To accommodate these various parameters, the methodology could be adjusted in several ways. 1) The dollar-cost range could be extended over additional orders of magnitude. 2) The low-end cost range could be raised or eliminated to provide a category for risks that are not of concern, while still realistically resolving other levels of risk in ways that are meaningful for prioritizing, planning, and funding corrective actions. Since only a relative, but consistent and meaningful, ranking of risk is needed, this might be accomplished by re-normalizing the range of risk (in dollars or arbitrary units), and/or adding more risk levels and refining their definitions to obtain useful distinctions for planning and implementing a protection program. Risk assessment is an iterative process that should always include reality checks to assure that the ranking process generates groups of risks that are meaningfully different and practically distinguishable.

Range of Risk

The risk for each threat group is determined by applying the numerical values to each level of threat, vulnerability, and consequence. The relative numerical ranges discussed above for each element gives a risk range from 10^4 to 10^8 in arbitrary units. Risks scoring below 10^5 are labeled Routine and are colored green. Risks between 10^5 and 10^6 are labeled Low and colored yellow. Risks with values between 10^6 and 10^7 are labeled Critical and are colored purple, and those greater than 10^7 are labeled Catastrophic and are colored red. Each risk category is distinguished from its neighbors by a factor of 10. In applying this evaluation to a real facility, the analysts must take care that there are real distinctions among the groups (levels), but within a group no distinction should be expected to be meaningful. The risk results identified at a particular facility can be displayed in a colored matrix and are relative only to each other; comparisons cannot be made to other facilities or locations.

10.9 Application of SRA Results

Evaluations of existing, proposed, or new enhancements to security now can be gauged against the relative risks described by the colored matrix. Under constrained resources, this approach has several advantages. It is rational and systematic. It also is self-correcting because as upgrades are completed in a particular area to reduce vulnerability, that area will rank lower in the overall risk ranking and, hence, will not be scheduled for further upgrades. In addition, each ranking draws attention to a particular set of adverse actions and the associated vulnerabilities and protective systems. Security upgrades not only to reduce vulnerability but they also can deter adversaries, thereby reducing the contribution from the threat element. For example, certain groups are known to avoid guarded facilities.

The relative risks in the red or High category are deal with first to determine if corrective actions or compensatory measures should be applied to reduce the risk. Risk management must consider the relative risk to the target, the cost of mitigating the damage, and the extent of willingness to accept certain levels of risk. In assigning values using the vulnerability matrix, consideration is taken of existing protective actions, such as the presence of an armed protective force, physical-access controls, alarm systems, investigations of personnel's' backgrounds, training and awareness programs, and security inspections. The response capabilities of the LLEA can be taken into account, provided that effective communications can be assured at all times. Protective measures taken by the vendors with whom the facility does business also can be included. For example, vendors who deliver HPMs to a chemical process facility may carry out background investigations of their delivery personnel, and certify and identify to their customers those whose checks were satisfactory. Alterations of any existing conditions that affect the protective systems would necessitate another assessment of the risk.

Before moving to illustrative examples of the risk-element matrices, we make some simple observations about the overall risk pattern. Any enhancement or decline in security measures likely will affect more than one scenario. All terms in the matrix must be considered in evaluating the effects of augmenting or decreasing a security measure. Some measures might be of low enough cost that even if they affect only the medium-risk scenarios, they might be considered reasonable to implement. The analysis should not end after considering only the high-risk scenarios. Probably, the reduction of a high risk also will moderate some of the medium risks.

Individual Risk-element Matrices for a Sample Facility

In a risk assessment, risk evaluation matrices are completed for each risk element versus each target type. The process is illustrated here for targets that might be found at a production facility. Each member of the risk-evaluation team might fill out matrices of the type below. The individual assessments then would be discussed and merged to arrive at an overall evaluation for the facility.

Threat Matrix

TARGET TYPE	THREATS									
Adversary →	**T**	**C**	**P**	**DE**	**VA**	**IC**	**M**	**I**	**V**	**Comments**
HPM Storage Facilities										
Tube Truck Station										
Production Equipment										
Property Storage Areas										

THREAT (ADVERSARY) CODES:

T	=	Terrorists
C	=	Criminals - White Collar and Common
P	=	Psychotics
DE	=	Disgruntled Employee or Visitor
VA	=	Violent Activists
IC	=	Intelligence Collector / Industrial Spy
M	=	Militia/Paramilitary Groups
I	=	Insiders
V	=	Vandals

A threat is an adversary with specific objectives in relation to a target. In considering threats, specific numbers and capabilities were considered but not specifically listed in the descriptions and definitions of this report to protect sensitive security-related information.

CATEGORIZATION LEVEL:

L = Low. Not likely to threaten. Adversary is not present in the geographic area or not active. Few, if any, incidents or attempts have occurred and none recently.

M = Medium. A malevolent operation is possible. Incidents have occurred or been attempted at the facility or in the immediate geographical area.

H = High. Strong possibility of malevolent action over time. Frequent or serious incidents have occurred or been attempted at the facility or in the immediate geographic area.

Vulnerability Matrix

TARGET TYPE	**VULNERABILITIES**									
Adversary →	**T**	**C**	**P**	**DE**	**VA**	**IC**	**M**	**I**	**V**	**Comments**
HPM Storage Facilities										
Truck Unloading Station										
Production Equipment										
Property Storage Areas										

THREAT (ADVERSARY) CODES:

T	=	Terrorists
C	=	Criminals - White Collar and Common
P	=	Psychotics
DE	=	Disgruntled Employee or Visitor
VA	=	Violent Activists
IC	=	Intelligence Collector / Industrial Spy
M	=	Militia/Paramilitary Groups
I	=	Insiders
V	=	Vandals

A vulnerability is a weakness or susceptibility in the system that, if exploited, could cause an undesired result or event. If there is a potential for damaging national security, the vulnerability may be classified provided that the information available about it is sufficiently specific to allow its exploitation.

CATEGORIZATION LEVEL:

L = Low. No readily exploitable vulnerabilities apparent. An adversary would require extensive effort and/or time to complete a successful attack.

M = Medium. Successful exploitation of existing vulnerabilities may degrade operation. An adversary would need to plan the attack to thwart protective measures. The invader may encounter defensive measures before completing the malignant act.

H = High. Major vulnerabilities exist that are not entirely mitigated by protection measures. An adversary can exploit these vulnerabilities before detection and intervention are effective.

Consequences Matrix

TARGET TYPE	CONSEQUENCES									
Adversary →	**T**	**C**	**P**	**DE**	**VA**	**IC**	**M**	**I**	**V**	**Comments**
HPM Storage Facilities										
Truck Unloading Station										
Production Equipment										
Property Storage Areas										

THREAT (ADVERSARY) CODES:

T	=	Terrorists
C	=	Criminals - White Collar and Common
P	=	Psychotics
DE	=	Disgruntled Employee or Visitor
VA	=	Violent Activists
IC	=	Intelligence Collector / Industrial Spy
M	=	Militia/Paramilitary Groups
I	=	Insiders
V	=	Vandals

CATEGORIZATION LEVEL:

N = Negligible (loss, cleanup costs <$10,000). This will not result in injury, occupational illness, or damage to systems ; the costs of cleanup and environmental restoration are negligible;

M = Marginal (loss, cleanup costs $10,000-$100,000). This may cause minor injury, occupational illness, or system damage; there will be some costs for cleanup and environmental restoration ;

C = Critical (loss, cleanup costs $100,000-$1 million). This may cause severe injury or occupational illness; the expenses of cleanup and environmental restoration will be significant ;

K = Catastrophic (loss, cleanup cost >$1 million). This may cause death or loss of systems , shutdown of the plant with the associated severe economic loss; there will be major costs for cleanup and environmental restoration.

Summary Matrix

The risk to each target group is determined by applying mathematical functions to each of the three risk elements, namely threat, target vulnerability, and consequence. The risks are categorized into four levels; High (red), Medium (purple earlier this was called violet), Low (yellow), and Routine (green), relative only to each other. Comparisons cannot be made to other facilities or locations because the data are mostly empirical and provided by persons knowledgeable of the assets and threats at this location. The relative risks in the red category (High) are addressed first to determine if corrective actions or compensatory measures should be applied to reduce them. Risk management must consider the relative risk to the target, the cost of mitigating it, and the willingness to accept a certain level of risk. The identification of risks must also account for existing protective measures, such as the activities of an armed protective force, physical- and cyber-access controls, alarm systems, personnel's background investigations, training and awareness programs, and self inspections. Any alterations of the existing factors would necessitate another assessment of the risk. The table below is a sample of a summary matrix.

Summary Matrix

Targets	Risk Elements	Terrorist	Criminal	Psychotic	Disgruntled Employee	Violent Activists	Intelligence Collector	Militia	Insider	Vandal	Comments
HPM Storage Facilities	Threat	M	L	M	H	M	L	L	H	M	
	Vulnerability	H	M	L	H	M	L	H	M	M	
	Consequences	C	L	M	C	M	N	C	M	N	
Truck Unloading Station	Threat	M	L	M	H	H	L	L	H	H	
	Vulnerability	H	M	L	H	H	L	H	H	H	
	Consequences	K	L	M	K	K	N	K	M	M	
Production Equipment	Threat	M	L	M	H	M	H	L	H	L	
	Vulnerability	H	M	M	H	M	M	M	H	M	
	Consequences	K	M	M	C	C	C	C	M	M	
Property Storage Areas	Threat	L	H	M	H	H	L	L	H	M	
	Vulnerability	H	M	L	H	M	L	H	H	H	
	Consequences	M	M	M	M	M	N	M	M	M	

Corrective actions of various types could lower the overall risks and this is the purpose of the analysis. Table 10.2 is a checklist of protective actions that could reduce vulnerabilities at a facility. Table 10.3 is a checklist for the process of planning the protection program.

Table 10.2. Protective Measures Check List

- On-site protective force
- Local law enforcement agencies
    - Communications
    - Response
- Perimeter systems
    - Fence (single/double with exclusion zone)
    - Intrusion sensors
    - Assessment systems
    - Visual and small arms barrier (truck station)
- Vehicle portal
    - Vehicle-access control
    - Double gate with movable crash-through barrier
    - Vehicle barriers in fences to prevent crash through (e.g., anchored cable)
    - Searches for explosives and weapons
- Vehicle barriers near target areas
    - Movable barriers at gate or portal
    - Semi-permanent or permanent barriers to keep vehicles at adequate distance
- Vendor qualification program
    - Vendor checks background of its delivery personnel
    - Vendor vehicles escorted onsite
- Intrusion detection systems
    - Door alarms
    - Space alarms
    - Window
        - Elimination might improve security.
        - Intrusion-detection measures
    - Assessment capability (e.g., video)
- Access controls
    - Key locks
        - Key-control program
    - Badge reader
    - Biometric identification system
    - Personnel portal monitors for metal, explosives, special nuclear materials
    - Equipment portal
        - Screening equipment
        - Inspection by security personnel
    - Two-person rule
        - Two persons require for access to, and work in, sensitive areas
- Personnel protection programs

- Background checks and periodic updates
- Substance monitoring program

Security awareness and training programs

Operations security (OPSEC) program

- The OPSEC program provides information security rather than physical security, but information about the facility's protective systems should be protected.

Integration of plant safety, process safety, and protective systems

- Safe storage of hazardous materials
- Minimum quantities near occupied areas
- Safety-related equipment and their vital systems have been identified and protected

Table 10.3. Checklist for Planning the Protection Program

- Security Plan
  - Threats specified
  - Targets identified
  - Protection elements and vulnerabilities identified
  - Consequences understood
  - Accepted risk documented
- Other plans
  - Information Security plan
  - OPSEC plan
  - Cyber-security plan
- LLEA arrangements documented
  - Police
  - Fire
  - Local FBI, ATF
- Secure communications
  - Onsite
    - Transmitter coverage
    - Backup antenna
  - To Local Law Enforcement Agencies (LLEA)
- Testing programs
  - Individual protection elements
  - Integrated exercises
    - Tabletop assessments
    - Limited scope performance-testing
    - Full field exercise
- Emergency Operation Center (EOC)
  - Secure location - away from targets
  - Alternative (backup) location
  - Equipment
  - Personnel assignments
- Security plan review
  - Documentation
  - Schedule
- Security Awareness Program
  - Security awareness training for employees
  - Security awareness reminders
- Documentation
  - Security Plan
  - Vulnerability Assessments
  - Agreements with LLEA, fire support
  - Results of performance tests
  - Corrective-action tracking
  - Emergency operations plan
  - Building and Site evacuation plan

11. DATA SOURCES AND COMMENTS ON DATA QUALITY

One of the more challenging aspects of conducting quantitative hazards analysis is the derivation of quality reliability data, which is used for component failure rate estimation. It is a rare case that a facility will have developed comprehensive failure data on its' system components such that an accurate estimation of the individual failure rates can be determined. In most instances, order-of-magnitude engineering estimates are made which are based on institutional knowledge of system performance, or are loosely based on industry average data tables. Caution should be exercised when using industry average data, as it is unlikely that a facility operating parameters (environmental conditions, maintenance policy, operational stresses, initial component quality, etc.) will match those of equipment sets from which industry average data is derived. It is prudent practice for the analyst to carefully review this data, preferably with input from equipment, process and systems engineering and operations experts, and to modify the data to more closely approximate field conditions and operational history of the facility. Once this data evaluation and adjustment exercise is done, consistent use of these component values will provide consistency and credibility to future analyses for similar systems within the facility.

Even when a facility has captured equipment reliability data specific to its' operations, careful analysis should be conducted to determine if this data represents expected function over the life of the facility or system being studied. For example, no field failures of a component over a few years of system operation, where the expected system life is many years, does not necessarily indicate high reliability of that component. An excellent discussion of equipment reliability and data quality is provided by I. Sutton in the text “Process Reliability and Risk Management, Chapter 7”. (Reference 9).

The following graph shows the general hierarchy of data quality.

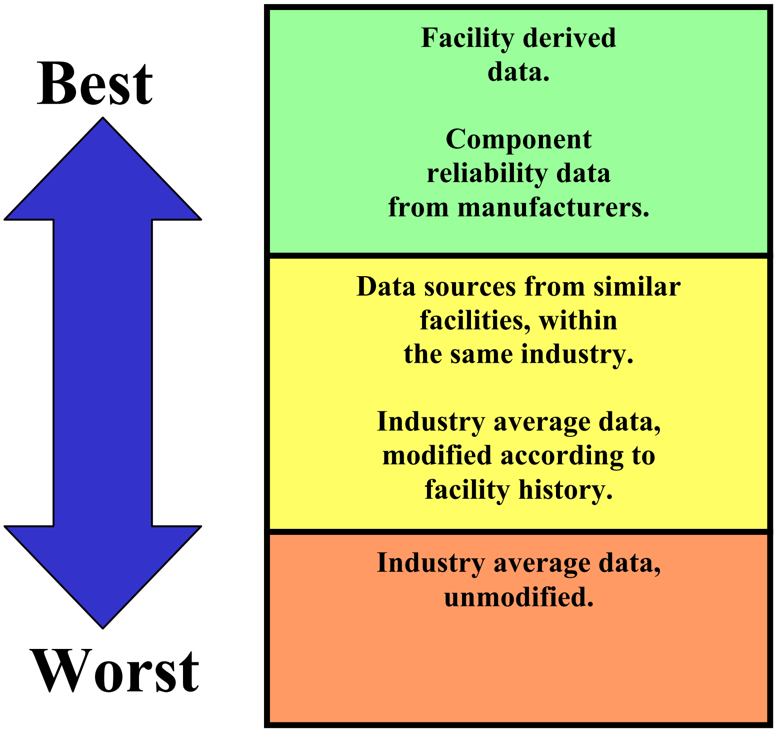

Best
Worst
Facility derived data.
Component reliability data from manufacturers.
Data sources from similar facilities, within the same industry.
Industry average data, modified according to facility history.
Industry average data, unmodified.

Figure 10.1: Sources of Data – Data Quality

Documentation of the PHA results is important to assure that a systematic and thorough analysis of potential hazards was conducted, and to have a permanent record for compliance purposes, risk-based decisions and third-party evaluations. Documentation is also necessary to follow up on the implementation of recommended actions and to enable productive updates.

12. DISCUSSION

It is of the utmost importance for the future of the PV industry to prevent accidents that could jeopardize the workers' safety or pollute the environment. Furthermore, since an accident could cause a facility to become inoperable or have to be closed, the programmatic impact and loss of production should be weighed in. For facilities that use hazardous materials in forms and quantities that can cause harm, Process Hazard Analysis (PHA) is recommended to identify potential accident initiating events so that they can be prevented or mitigated. PHA methods range from the simple Checklist or What if analyses that require only a few hours of meetings to the very comprehensive FMEA or FTA that require a few months of effort. The later are justified for complex systems or when potential consequences are unacceptable. A major output of hazard analysis is the identification of design or facility modifications that could increase safety or security in such a facility. Frequently, hazard analysis also helps in improving system reliability and preventing production loss.

This reference guide outlines the basics of the different methods of hazard analysis and outlines illustrative examples of their use. For each example, we discuss lessons learnt and cost and benefits of undertaking such analysis. In all the cases that we have been involved the benefits by far surpassed the associated costs.

ACKNOWLEDGEMENT

This work was supported by the U.S. Department of Energy, Solar Energy Technologies under contract DE-AC02-76CH00016.

REFERENCES

Fthenakis V., Multilayer Protection Analysis of Photovoltaic Manufacturing Facilities, Process Safety Progress, 20(2), 2001.

Hazard Analysis Guide, International Sematech, Tech Transfer#99113846A-ENG, November 1999.

HAZOP, Guide to Best Practice, Institution of Chemical Engineers, UK, 2002.

CCPS (1992), Guidelines for Hazard Evaluation Procedures, American Institute of Chemical Engineers, 1992.

Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry, International Sematech, Tech Transfer#92020963A-ENG, September 30, 1992.

Sutton I., Process Hazard Analysis, SW Books, Houston, TX, 2001

Lemley R., V.M. Fthenakis V.M. , and Moskowitz P.D.

Moskowitz P.D., Fthenakis V.M., Crandal R. and Nelson B., Analyzing Risks Associated with Hazardous Production Materials, Solid State Technology, 137(7) , 121-126, 1994.

Sutton, I.S. 1992. *Process Reliability and Risk Management,* New York: Van Nostrand Reinhold.

CCPS (1989), *Guidelines for Process Equipment Reliability Data,* New York: American Institute of Chemical Engineers, Center for Chemical Process Safety.

CCPS (2001), *Layer of Protection Analysis, Simplified Process Risk Assessment,* New York: American Institute of Chemical Engineers, Center for Chemical Process Safety.

NPRD-95, *Nonelectronic Parts Reliability Data,* Rome, New York: Rome Laboratory, Reliability Analysis Center.

APPENDICES